Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

Data Processing Agreement

Regulations on data protection and data processing

Shiftmove GmbH
Warschauer Straße 57
10243 Berlin

- hereinafter referred to as "Processor" -

and you

- hereinafter referred to as the "Controller" -

- hereinafter jointly referred to as the "Contracting Parties"

Preamble

This Data Processing Agreement ("DPA") pursuant to Art. 28 GDPR is part of our General Terms and Conditions ("Main Agreement") concluded between our users and Shiftmove GmbH and can be accessed here: **https://www.shiftmove.com/legal/agb**. According to this agreement, this DPA applies to the processing of your personal data in the context of the provision of our product.

By signing the order form, the Terms and Conditions, including this DPA, are deemed to be bindingly agreed upon, so that a separate signature of this DPA is generally not required.

Nevertheless, we provide our customers with the option to download the DPA separately, sign it, and return it to us. In this case, we kindly ask you to send a copy of the signed version to **privacy@shiftmove.com**.

The agreement is based on the provisions of the GDPR, the German Federal Data Protection Act (BDSG), and the Data Act.

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

§ 1 Subject matter, type and purpose of processing; type of personal data, categories of data subjects

(1) The subject matter of the processing is the provision of one or multiple services as a Software-as-a-Service from the Shiftmove Group ("Services"). The nature and purpose of the processing are defined in Annex 1a. The type of processing is listed in Appendix 1b.

(2) The categories of data subjects are defined in Appendix 1c.

(3) The type of personal data processed is defined in Appendix 1d.

(4) **Appendix 1** is part of this agreement.

(5) The Controller instructs the Processor to process this data for these purposes.

§ 2 Duration of the order

The duration of this order (term) corresponds to the term of the Main Agreement.

§ 3 Responsibility and authority to issue instructions

(1) The Controller shall be responsible for compliance with the provisions of data protection law, in particular for the lawfulness of the transfer of data to the Processor and for the lawfulness of the data processing (Art. 4 No. 7 GDPR). The Processor shall not use the data for any purposes other than those specified in this data processing agreement as well as the main Agreement and, in particular, is not authorised to pass them on to third parties not covered by § 6 of this agreement. Copies and duplicates will not be made without the knowledge of the Controller. Anything to the contrary shall only apply to the extent specified in § 3 (2) of this agreement.

(2) The Processor shall process personal data only on the documented instructions of the Controller, unless there is another obligation under Union law or the law of the Member State to which the Processor is subject. In the event of another obligation, the Processor shall inform the Controller of the corresponding legal requirements without delay prior to such processing, if legally permitted.

(3) The controller, but not the processor, is the data owner (see Recital 22 of the Data Act). The processor undertakes not to use any data transmitted by the controller (personal and non-personal data) for its own purposes, for profiling or for product improvement, unless the processor has been expressly permitted to do so. The processor thus fulfills the requirements of Art. 6 and Art. 8(2) of the Data Act.

(4) If the Processor is of the opinion that an instruction of the Controller violates data protection regulations, it shall inform the Controller immediately in accordance with Art. 28 (3) GDPR. Until the corresponding instruction has been confirmed or amended, the Processor is authorised to suspend the processing based on the violating instruction.

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

(5) Changes to the object of processing must be jointly agreed and documented. The Processor may only provide information to third parties or the data subject with the prior written consent of the Controller.

§ 4 Confidentiality

The Processor shall only give access to Controller personal data to employees who have been bound to confidentiality in accordance with Art. 28 (3) (b) GDPR and who have received dedicated training on the data protection provisions relevant to them. The Processor and any person subordinate to the Processor who has access to personal data may only process this data in accordance with the Controller's instructions, including the authorisations granted in this Data Processing Agreement, unless they are legally obliged to do so.

§ 5 Data security

(1) The contracting parties agree on the specific data security measures set out in **Appendix 2 "Technical and organisational measures"** to this agreement in accordance with Art. 28 (3) (c) GDPR in conjunction with Art. 32 (1) GDPR in order to ensure the security of the processing on behalf. The measures to be implemented by the Processor are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects within the meaning of Art. 32 (1) GDPR will be taken into account by the Processor when implementing such measures.

(2) **Appendix 2** is an integral part of this agreement.

(3) The Processor shall observe the principles of proper data processing. It shall guarantee the contractually agreed and legally required data security measures. The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. In doing so, the security level of the defined measures must not be undercut. Significant changes must be documented and communicated to the Controller in writing.

(4) In the event of a personal data breach, the Processor shall cooperate with and assist the Controller to enable the Controller to comply with its obligations under Art. 33, 34 GDPR, taking into account the nature of the processing and the information available to the Processor.

(5) In the event of a personal data breach in connection with the data processed by the Processor, the Processor shall notify the Controller without undue delay after becoming aware of the breach. This notification shall contain at least the following information:

- a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects affected and the approximate number of data records affected);

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

- contact details of a contact point where further information about the personal data breach can be obtained;
- the likely consequences and the measures taken or proposed to address the personal data breach, including measures to mitigate its possible adverse effects.

If and to the extent that not all such information can be provided at the same time, the initial notification will contain the information available at that time and further information will be provided as soon as it becomes available without undue delay thereafter.

§ 6 Inclusion of further Processors (subcontractors)

(1) For the purposes of this agreement, subcontractors are further Processors whose services are directly related to the provision of the main service. This does not include ancillary services which the Processor utilises, e.g. as telecommunications services, postal/transport services and cleaning. However, the Processor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure the data protection and data security of the Controller's data, even in the case of outsourced ancillary services.

(2) The use of subcontractors or the change of the existing subcontractor is permitted, provided that:

- the Processor notifies the Controller of such outsourcing to subcontractors 14 calendar days in advance in writing or in text form, and
- the Controller does not object to the planned outsourcing in writing or in text form to the Processor by the time the data is transferred.

(3) Should the controller object to a change of subcontractor within the objection period according to § 6 (2) the processor will check and inform the controller whether the service can be provided without the change of subcontractor. If, based on its review, the processor cannot provide the service without the change to the subcontractor, both parties shall have the right to terminate the contract in writing with a notice period of 14 days.

(4) A contractual agreement shall be concluded with the subcontractor in accordance with Art. 28 (3) and (4) GDPR.

(5) The transfer of personal data of the Controller to the subcontractor and the subcontractor's initial activities are only permitted once all legal requirements for subcontracting have been met. The subcontractors authorised by the Controller at the time the contract are listed in Appendix 3. The subcontractors of the subcontracting entities can be viewed under the links https://www.vimcar.de/legal/danteschutz/subunternehmer and https://www.avrios.com/de/legal/sub-Processors.

(6) Affiliated companies of the Shiftmove Group are commissioned as subcontractors.

(7) Any transfer of data processing to a third country requires the prior documented instruction or authorisation of the Controller and may only take place if the special requirements of Art. 44-49 GDPR are met.

(8) **Appendix 3** is part of this agreement.

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

§ 7 Rights of data subjects

(1) The Processor is obliged to support the Controller with appropriate technical and organisational measures, where possible, to comply with the obligations to respond to requests of data subjects exercising their rights under Art. 12 to 22 GDPR (Art. 28 (3) (e) GDPR).

(2) Insofar as the data subject has a right to data portability vis-à-vis the Controller, the Processor shall ensure that the Controller can receive the personal data processed in the Processor's area of responsibility in a structured, commonly used and machine-readable format.

(3) The Processor may only disclose, rectify, erase or restrict the processing of personal data in accordance with documented instructions from the Controller (Art. 28 (3) (g) GDPR).

(4) If a data subject contacts the Processor directly in order to exercise their rights pursuant to Art. 12 to 22 GDPR, the Processor shall forward the request to the Controller without undue delay.

(5) The Processor may only provide information to third parties or data subjects with the prior written authorisation of the Controller.

(6) The Controller is responsible for informing data subjects in accordance with Art. 12 and 13 GDPR. Necessary information in connection with this obligation, which is only available to the Processor, will be made available to the Controller upon request.

(7) The Processor shall assist the Controller, at the latter's request, in providing data in a structured, interoperable, and machine-readable format and, where applicable, in transferring it to third parties, insofar as the controller is held liable as the data owner of users in accordance with Art. 4ff. and Art. 8 of the Data Act.

§ 8 Obligations of the Processor

In addition to complying with the provisions of this contract, the Processor must comply with the obligations pursuant to Art. 28 to 36 GDPR. In this respect, the Processor shall in particular ensure compliance with the following requirements:

- If the Processor is legally obliged to appoint a data protection officer in writing in accordance with Art. 37 GDPR, § 38 BDSG, the Processor shall provide the Controller with the contact details of the data protection officer for the purpose of direct contact. The Controller must be notified immediately of any change of data protection officer.

- The external data protection officer at the Processor is

  clever datenschutz GmbH

  E-Mail: privacy@shiftmove.com

(2) The Processor shall support the Controller in complying with the obligations set out in Art. 32 - 36 GDPR regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes in particular

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

- ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a potential breach through security vulnerabilities and enable the immediate detection of relevant breach events
- the obligation to inform the Controller without undue delay if the Processor becomes aware of a personal data breach (Art. 28 (3) (f), Art. 33 (2) GDPR);
- the obligation to support the Controller in the context of his duty to inform the data subject and to provide him with all relevant information in this context without delay;
- the support of the Controller for its data protection impact assessment;
- the support of the Controller in the context of prior consultations with the supervisory authority.

(3) Any transfer of data by the processor to a third country or an international organisation shall be carried out exclusively in compliance with the legal requirements for the transfer of data to third countries in accordance with Art. 44ff. GDPR. In order to ensure an adequate level of data protection, the processor shall only transfer data to recipients in third countries if an adequacy decision of the EU Commission exists for the third country in question (Art. 45 of the GDPR), appropriate safeguards for the transfer, such as standard contractual clauses, are in place (Art. 46 GDPR) , internal data protection regulations (Art. 47 GDPR) or other exceptional circumstances for the transfer of data (Art. 48 GDPR). The controller consents to the transfer of data to subcontractors from §6 (5) of this agreement, who may be based in third countries.

(4) The Processor shall support the Controller in fulfilling its obligations regarding data portability and switching providers in accordance with the requirements of the Data Act and shall provide information on supported formats and interfaces in accordance with Articles 23-29 of the Data Act.

§ 9 Control rights of the Controller, Art. 28 para. 3 sentence 2 lit. h GDPR

(1) The Processor undertakes to provide the Controller, upon written request and within a reasonable period of time, with all information and evidence necessary to carry out a written inspection.

(2) Audit and Inspection Rights of the Controller

The Controller shall have the right, prior to the commencement of processing and regularly thereafter, to verify compliance with the technical and organizational measures implemented by the Processor.

This shall primarily be carried out through:

- obtaining information from the Processor; and/or
- the submission of independent audit reports or recognized certifications.

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

a) Event-Related On-Site Inspections

The Controller shall be entitled to carry out an on-site inspection at the Processor's premises if:

- there are specific indications giving rise to doubts about the accuracy or completeness of the submitted audit reports or certifications,
- a security incident within the meaning of Art. 33 (1) GDPR has occurred in connection with the data processing, or
- the documents provided do not sufficiently evidence the required safeguards.

In such cases, on-site inspections must generally be notified in writing at least 14 calendar days in advance.

A shorter notice period shall only be permissible in duly justified exceptional cases, where urgency directly results from the respective event (e.g., in the case of a security incident). In such cases, the Controller shall provide a comprehensible justification for the shortened notice period and, upon request, furnish evidence thereof to the Processor.

b) Non-Event-Related On-Site Inspections

Irrespective of any specific event, the Controller may conduct one non-event-related on-site inspection per calendar year.

Such inspections must also be notified in writing at least 14 calendar days in advance.

c) General Provisions

The exercise of inspection rights shall not unduly disrupt the Processor's business operations or be exercised in an abusive manner.

The Controller shall bear any actual costs incurred by the Processor as a result of non-event-related on-site inspections.

(3) The Controller shall be obliged to prepare a written record of each inspection carried out. Any deviations, deficiencies, or other material findings identified in the course of the inspection shall be communicated to the Processor without undue delay, and in any case within a reasonable period following completion of the inspection, in text form. The inspection record shall be made available to the Processor upon request.

§ 10 Liability

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

(1) The liability of the parties shall be governed by Art. 82 GDPR. This shall not affect the Processor's liability to the Controller for breach of obligations under this contract or the main contract.

(2) The parties shall release each other from liability if one party proves that it is not responsible in any respect for the circumstance that caused the damage to a data subject. § 10 (2) sentence 1 shall apply accordingly in the event of a fine imposed on a party, whereby the indemnification shall be made to the extent that the respective other party bears a share of the responsibility for the breach sanctioned by the fine.

§ 11 Non-compliance with the clauses and termination of the contract (Art. 28 (3) (g) GDPR)

(1) Without prejudice to any provisions of the GDPR, in the event that the Processor is in breach of its obligations under these Clauses, the controller may instruct the Processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The Processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(2) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

- the processing of personal data by the Processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
- the Processor is in persistent breach of these Clauses or its obligations under the GDPR;
- the Processor fails to comply with a binding decision of a competent court or the competent supervisory authorities regarding its obligations pursuant to these Clauses or the GDPR.

(3) The Processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(4) Upon completion of the provision of the processing services, the Processor shall either delete or return all personal data at the discretion of the Controller, unless there is a legal obligation to store the personal data or the Controller requests access pursuant to section 2.1.5 of the General Terms and Conditions.

(5) In this case, the Processor shall confirm to the Controller in text form, stating the date and without further request, that it has returned to the Controller or destroyed or securely erased all data carriers and other documents that may have been provided to it and has therefore not retained any data of the Controller.

(6) Documentation that serves as proof of proper data processing shall be retained by the Processor beyond the end of the contract in accordance with the respective retention periods.

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

§ 12 Final provisions

(1) Data carriers and data records provided shall remain the property of the Controller.

(2) Should one or more provisions of this agreement be invalid, this shall not affect the validity of the remaining provisions. In the event of the invalidity of one or more provisions, the contracting parties shall immediately replace the invalid provision with a provision that most closely corresponds to the invalid provision in economic terms and in terms of data protection law.

(3) The contracting parties agree that Processor's defense of the right of retention within the meaning of § 273 BGB (German Civil Code) with regard to the data to be processed and the associated data carriers is excluded.

(4) There are no oral side agreements between the parties. Any amendment, supplement, or termination of this agreement requires written form in order to be valid, which may itself only be waived in writing. Compliance with the written form requirement is satisfied by a signature executed with at least a simple electronic signature recorded via e-signature software. The electronic signature has full probative value.

(5) Insofar as other agreements at the time of the conclusion of this contract contain provisions to the contrary or contradict this contract, the contents of this contract shall take precedence.

(6) The following annexes form an integral part of this agreement: Appendix 1 "Information on processing", Appendix 2 "Technical and organisational measures", Appendix 3 "Subcontractors".

Company:	
Address:	
Date:	
Place:	
Name:	
Signature of Controller	

Company:	Shiftmove GmbH
Address:	Warschauer Str. 57, 10243 Berlin
Date:	15.09.2025
Place:	Berlin
Name:	i.V. John Maik Ryssel
	Signed by: i.V. John Maik Ryssel 4ABB00F788844C5...
Signature of Processor	

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

Appendix 1

Information on processing

The information set out below regarding the subject matter and purpose of the processing, the types of processing, the categories of data subjects, and the categories of personal data processed relates to the full potential scope of the services offered by the Processor. Binding, however, are solely those purposes, types of processing, categories of data subjects, and categories of personal data which arise from the Main Agreement, including the respective Order Form, and which are required for the products and functionalities actually ordered by the Controller.

a) Object and purpose of the processing

The subject of the processing is the provision of one or more of the following services as Software-as-a-Service:

- Software for fleet management (Avrios) including the purposes:
  - Management of vehicles and drivers
  - Management of fines
  - Administration of fuel cards
  - Management of damage reports
  - Carrying out driver's license checks
  - Creation of reports and analyses

- Live localisation and route documentation (Vimcar Fleet Geo) including the purpose:
  - Live tracking of vehicles
  - Route documentation of vehicles
  - Geo-fencing notification for vehicles

- electronic logbook (logbook) including the purposes:
  - Route documentation of vehicles
  - Export of logbook data

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

b) Type of processing

As part of the assignment, the Processor will carry out the following types of processing in accordance with Art. 4 No. 2 GDPR: Collection, recording, organization, ordering, storage, adaptation, alteration, retrieval, consultation, transmission, restriction, erasure and destruction of data.

c) Categories of data subjects and personal data

When providing the services, personal data of the following categories of data subjects may be processed on a regular basis:

1) Drivers (former and current employees and their spouses and dependants, current contractors as well as applicants, candidates and future employees);
2) Users (authorised users of the customer (who are not drivers) who are entitled to use the services);
3) Third parties (customers, business partners, suppliers, consultants, representatives, freelancers and/or subcontractors of the customer (natural persons)).

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

d) Type of data processed

Avrios fleet management:

- Tasks and comments
- Fine notice information (addressee, amount, photos)
- Entry date and exit date
- Vehicle information (CO2 emissions, damage reports, license plate, chassis number)
- Photos (driving license photos and portrait photos)
- Driving license information
- Contact information (telephone number, fax number, cell phone number, e-mail address)
- Personal master data (first name, surname, address, gender, date and place of birth, language, nationality, residence permit, marital status, details of dependents, national identification number)
- Company administration data (internal ID, cost centre, organization, department, location, sector and sub-sector, reporting structure)
- Information on salary planning (fringe benefits relating to company cars), service specifications and associated information (entitlement to company car and class of company car)
- Fuel card information (provider, costs, date, product)
- Accident prevention regulation test results
- Device data and IT usage data

Vimcar Fleet Geo:

- First name, last name
- E-mail address, telephone number, cell phone number
- Logbook data
- Trip data during the journey
- Live tracking and route documentation;
- VIN (Vehicle Identification Number)
- Verification information for carrying out the automated driver's license check (optional when using the driver's license check)
- Technical vehicle data (e.g. repair status), photos of vehicles (optional when using the damage management system)
- Device data and IT usage data

Vimcar Logbook:

- First name, surname
- E-mail address, telephone number, cell phone number
- Logbook data
- Trip data during the journey
- Start and end point of trips

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

- Kilometers driven
- Categorization of private and business trips
- Contact and address data
- VIN (Vehicle Identification Number)
- Test parameters for carrying out the automated driver's license check (optional when using the driver's license check)
- Technical vehicle data (e.g. repair status), photos of vehicles (optional when using the damage management function)
- Device data and IT usage dat

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

Appendix 2

Technical and Organisational Measures according to Art. 32 (1) GDPR

1. Measures to ensure confidentiality

1.1 Entrance control

Is intended to prevent unauthorised persons from gaining physical access to data processing systems. Measures for building and room security..

- (Documented) building securtity concept
- Locking system
- Burglar-resistant windows & doors
- External security service
- Alarm system
- Link between alarm system and security service/police
- Light barriers/ motion detectors
- Connection of motion detectors to security service/ police
- CCTV surveillance
- Access control concept
- Biometric access control
- Person verification at gatekeeper/reception desk
- Logging of visitor accesses / visitor book /visitor badges
- Personal supervision of external persons in security areas
- ID badges
- Electronic access code cards/ access transponders
- Security zones (visitor meeting, server rooms, workplaces, research)
- Existence of an authorisation overview for the security zones
- Self-closing doors are used when zones are crossed
- Authorisation cards (for individual zones)
- Key regulations
- Separately secured entrance for arrivals and departures
- Separately secured access to the server room
- Separately secured access to the computer centre
- Careful choice of cleaning staff
- Work instructions/guidelines regarding the locking of rooms when leaving/finishing work

1.2 Access control

Intended to prevent unauthorised access to and use of data processing systems. System security.

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

- Role-based security concept/ assignment of user rights
- Creation of user profiles
- Authorisation management
- Avoidance of group identifiers
- Documented process for assigning rights when new employees join the organisation
- Documented process for withdrawing rights when employees change departments
- Documented process for withdrawing rights when employees leave the company
- Functional and/or time-limited assignment of user authorisations
- Use of individual passwords
- Login with user name and password
- Login with biometric data
- Separate BIOS password
- Automatic password-secured locking of the screen after inactivity (screen saver)
- Privacy screens for potential unauthorised viewing
- Password policy with minimum password complexity requirements:
    - Minimum of 8 characters
    - Minimum of 12 characters for local admin passwords
    - Upper and lower case, special characters, number (of which at least 4 criteria)
    - Prevention of trivial passwords (e.g. password1, password2, 123456, qwerty)
    - Password history (no re-use of last passwords)
    - Prevention of PW after positive matching with dictionaries
    - Input restriction of certain special characters to prevent SQL injections
    - Appropriately secure PW reset procedure
- Change cycle for passwords:
- Time delay between login attempts
- Failed login attempts are displayed to users
- Automatic blocking of user accounts after multiple incorrect PW entries
- Blocking passwords after security incident and reassignment
- Blocking passwords in case of suspected infringement
- Largely automatic (technical) implementation of the password policy
- Two- or multi-factor authentication for high-risk processes
- Save passwords in browser only with master password
- Access to websites is managed restrictively
- Other: (e.g. use of Fido2)
- Hashing of stored passwords using up-to-date hashing methods:
    - Used hashing method:
    - Hashes are "salted" and/or "peppered"
- Encryption of networks
    - Encryption algorithms used: SSH, HTTPS, TLS 1.2+,
- Locking of data processing equipment (e.g. locked cage for servers).
- Deactivation of autostart of external media
- Programme check and release procedures for new installations
- Preventing the execution of downloaded software whose sources are marked as insecure
- Preventing automatic execution of programmes from temporary downloads
- Use of intrusion prevention systems

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

- Use of VPN technology
- Use of anti-virus software: server
- Use of anti-virus software: clients
- Use of a software firewall
- Use of a hardware firewall
- Central collection of malware alerts
- Default authentication information changed after software installation/first login
- Central device management
- Mobile device management
- For smartphones: access only after authentication
- For smartphone: Use of biometric access methods only with exclusively local storage of biometric templates (within secure chips)
- For smartphone: Secure sources for apps, apps are tested and approved
- Storage of personal data/data carriers in lockable security cabinets or in separately secured rooms
- Policy on home office / teleworking
- Policy on private use of equipment or exclusion of private use
- Other measures:
    - Different passwords for different services or SSO
    - Use of a password manager

1.3 Access control

Shall prevent unauthorized activities in data processing systems outside granted authorizations

- Use of an authorization concept
- Minimal use of administrator accounts
- Different administrative roles according to least privilege concept (users, firewall, backups etc.)
- Superuser (e.g. root under Linux) not used as far as possible
- Regulation that surfing the Internet or reading/sending e-mails is not allowed using administrator privileges
- Use of own administration end devices (dedicated network connection)
- Separation of authorization approval (organizational) and authorization assignment (technical)
- Sending of telemetry data to manufacturers deactivated
- Regulation for restoring data from backups (who, when, on whose request)
- Storage of data backups (e.g., tapes, CDs) in an access-protected safe
- Regular review of roles and permissions
- Restriction of free and uncontrolled querying of databases
- Partial access to databases and functions (read, write, execute)
- Regular evaluation of logs (log files)
- Time limitation of access possibilities
- Deactivation of unused standard server services
- Logging at firewall level to detect unauthorized access between networks
- Automatic notifications when unauthorized processing is suspected
- Logging of remote maintenance accesses
- Logging of file accesses

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

- Logging of file deletions
- Logging of file changes
    - SPAM filter
- Intrusion detection (IDS)
    - Security Information and Event Management (SIEM) software
- Intrusion Prevention (IPS)
- Restricted access to log files (Log Admin only)
- Storage of log files on dedicated LogFile server
- Encrypted storage of data
- used encryption algorithms:
    - AES (128/256 bit)
    - 3DES
    - RSA (1024/2048 bit)
    - EC (256 bit)
    - Other: AES 256 AWS at rest Verschlüsselung
- Hash function used:
    - SHA2 (256, 384, 512 bit)
    - SHA3
    - bcrypt
- Other methods:
    - Hashes are "salted" (salt) or "peppered"(pepper)
- Two-factor authentication for web server maintenance
- SSL certificates only from trusted sources
- Controlled destruction of data:
    - Data media disposal - secure deletion of data media (DIN 66399)
    - Shredder (Cross-Cut, mindestens Stufe 3, DIN 66399)
    - Sealed metal containers (so-called data protection garbage cans)
    - Peter Gutmann algorithm - 35-fold overwriting
    - Physical destruction (e.g. shredder for particle sizes up to max. 1000 square millimeters)
    - Demagnetization by thermal destruction (heating of the magnetic disk surface beyond the Curie temperature of the coating used)
    - Demagnetization by means of a degausser
- Connection of branch offices or home offices only via VPN connections with client certificate authentication
- Use of WLAN only on current routers with effective access mechanisms
- WLAN guest access without access to internal network
- Data destruction policy
- Clean desk policy
- Checking incoming e-mails using anti-malware
- Security concept for handling printers, copiers, etc.
- Other measures:
    - Key storage via hardware security modules

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

2. 2 Measures to ensure integrity

2.1 Transfer control

Shall ensure the security of data during electronic transmission and data transport and the auditability of the transfer.

- How is data transmitted between the controller and third parties?
  - VPN connection
  - Secure File Transfer Protocol (sftp)
  - Citrix connection
- E-mail encryption:
  - SMIME
  - OpenPGP
  - Sending e-mails with encrypted ZIP files
- For messengers: transport and content encryption
- Data exchange via https connection
- Encryption protocol used:
  - TLS 1.2
  - TLS 1.3
- Encryption algorithms used:
  - AES (128/256 bit)
  - 3DES
  - RSA (1024/2048 bit)
  - Diffie-Hellmann
- Use of signature procedure
- Signature procedure used:
  - RSA
  - ElGamal
  - DSA
- Digital signing of macros
- No transmission of personal data (e.g. mail address) via HTTP GET request, as this data is stored in the web server log files and can be diverted by the website trackers used.
- For HTTPS: use of client certificates
- Encrypted requests to DNS services
- Regulation on the use of cloud services (incl. exit strategy)
- Documented management of data media, inventory control
- Encryption of confidential data records
- Encryption of mobile data carriers (e.g. laptop hard drives, external hard drives, USB sticks)
- Prohibition of carrying bags and other luggage as well as mobile phones into security areas
- Regulation on making copies of data records
- Making backup copies of data media that must be transported
- Documentation of the offices to which transmission is intended and the means of transmission
- Direct collection, courier service, transport escort
- Completeness and correctness check

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

2.2 Input control

The purpose is to ensure that it can be traced whether, who, and when personal data has been entered into data processing systems, changed or deleted.

- Technical logging of the entry, modification and deletion of data
- Manual or automated evaluation of the logs
- Differentiated user authorisations:
    - Individual user names, no user groups
    - Assignment of rights to enter, change and delete data based on an authorisation concept
    - Field access for databases
- Organisational definition of input responsibilities
- Commitment to data secrecy
- Log concept that goes beyond the OS standard
- Dedicated log server
- Regulation of access authorisations for log servers (LogAdmin)
- Regulation on retention periods for auditing/evidence purposes

3. Measures to ensure availability & resilience

3.1 Availability control

Designed to protect data against accidental destruction or loss.

- Fire alarm systems in server rooms
- Smoke detectors in server rooms
- Fire doors
- Waterless fire suppression systems in server rooms
- Water sensors in server rooms
- Lightning / overvoltage protection
- Air-conditioned server rooms
- Server rooms in separate fire compartment
- Storage of backup systems in separate rooms and in separate fire compartment
- Server rooms not under or next to sanitary facilities
- Access to server rooms limited to necessary personnel only
- Alarm signal in case of unauthorised access to server rooms
- Storage of archive storage media under necessary storage conditions (air conditioning, protection requirements, etc.)
- CO2 fire extinguishers in the immediate vicinity of the server rooms
- UPS system (uninterruptible power supply)
- Power generator
- Fireproof cabinets
- Data protection safe
- Documented data protection and backup concept

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

- Execution of data backups and creation of backups according to the 3-2-1 principle
- Emergency archive (outsourcing of data)
- Regular tests for data recovery
- At least one backup system cannot be encrypted by malicious code
- Mirroring of hard disks (e.g. RAID)
- Separate partitions for operating system and data
- Emergency plan in place (BSI standard 200-4)
- Regular review of the emergency plan through testing and emergency exercises
- Ensure long-term technical readability of backup storage media.

3.2 Resilience (resilience and failure control)

Shall enable systems to cope with risk-related changes and to demonstrate tolerance and compensatory capacity in the face of disruptions

- Redundant power supply
- Redundant data connection
- Redundant air conditioning
- Backup data centres available (hot or cold stand-by?): Cold
- other redundant systems/procedures:
- Use of a highly available SAN solution (Storage Area Network)
- Computer Emergency Response Team (CERT)
- Use of load balancing
- Delimitation of critical components
- Carrying out penetration tests
- System hardening (deactivation of unnecessary components)
- Immediate and regular activation of available software and firmware updates
- Regularly checking the configuration of the firewalls
- Regular sensitisation of employees (at least annually)
- Process for immediate reporting of incidents to IT is known to all employees

4. Measures for regular review, assessment and evaluation

4.1 Control procedures

Shall ensure the effectiveness of data security measures

- Processing directories (Art. 30 I and II DSGVO) are updated annually
- Notification of new/modified data processing procedures to the data protection officer
- Notification of new/modified data processing procedures to the IT Security Officer
- Processes for reporting new/changed procedures are documented
- Regular review and evaluation of the software used
- Concepts and documentation are regularly reviewed (PDCA cycle)
- Review of the effectiveness of security measures taken at least annually

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

- Conduct security tests on web applications according to good practice procedures (e.g. OWASP Testing Guide)
- If findings are made during the aforementioned review, the security measures are adjusted in line with the risk.
- Process exists for responding to security breaches (attacks) and system malfunctions (incident response management)
- Documentation of security incidents
- Security certifications (ISO 27001, BSI IT-Grundschutz, ISIS12 etc.)
- Use of security intelligence (real-time analysis; log management, SIEMs, NBADs, network forensics)

4.2 Order control

Shall ensure that data processed on behalf by service providers (subcontractors) are only processed in accordance with the principal's instructions.

- Contract design in accordance with legal requirements (Art. 28 DSGVO)
- Central registration of existing service providers (uniform contract management)
- Pre-contract checks at the contractor's premises before the start of the contract
- Regular checks at the contractor's premises after the start of the contract (during the term of the contract)
- On-site inspections at the contractor's premises
- Review of the contractor's data security concept
- Review of existing IT security certificates of the contractor
- Contractor has appointed data protection officer

4.3 Separation control

Data collected for different purposes shall also be processed separately.

- Separation of clients (multi-client capability of the system used).
- Physical data separation (e.g. different systems or data carriers)
- Logical data separation (e.g. based on customer or client numbers)
- Data backups of client data on separate data carriers (without data of other clients)
- Authorisation concept that takes into account the separate processing of client data from data of other clients
- Separation of development, test and production systems
- Assignment of data records to purpose attributes
- For pseudonymised data: Separation of the assignment file & storage on a different system

4.4 Other data protection or security management

- Appropriate organisational structure for information security with clearly defined roles
- IT security officer appointed
- Use of data protection management software
- Data protection officer appointed

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

- Documented process for handling IT security incidents
- Documented process for handling data protection incidents
- Clear responsibilities for handling data protection and security incidents
- Documented process for ensuring data subject rights
- Central storage of policies/processes/procedural instructions accessible to all employees
- Guidelines/processes/procedural instructions are communicated within the company and known to all employees.
- External service providers are bound to secrecy, if necessary.
- Arrangements for effective data deletion on hardware that is taken back by the manufacturer or service provider
- Regular training on the guidelines and security processes

Docusign Envelope ID: CB35CF7C-177A-4D18-82C4-57AC107AA016

Annex 3

Subcontractors

The Controller has authorized the use of the following sub-Processors:

1	**Name:**	Vimcar GmbH
	Address:	Warschauer Str. 57, 10243 Berlin, Germany
	Contact:	datenschutz@vimcar.com
	Third Country:	No
	Purpose:	• Provision and development of the SaaS Vimcar Logbook and Vimcar Fleet Geo • customer support • freight and package distribution
2.	**Name:**	Avrios International AG
	Address:	Rieterstr. 6, 8002 Zurich, Switzerland
	Contact:	privacy@avrios.com
	Third Country:	Yes
	Guarantee:	Adequacy decision of the EU Commission
	Purpose:	• Provision of the SaaS Avrios Fleet Management • Customer support