Contract for commissioned processing pursuant to Art. 28 GDPR

Agreement

between

Munksøgård Delebilforening
Munksøgård 21A
DK-4000 Roskilde

- Person responsible - hereinafter referred to as the client -

and

Digital Mobility Solutions GmbH
Vaalser Street 17
52064 Aachen

- Processor - hereinafter referred to as Contractor

Infobox

The individual provisions pursuant to Art. 28 (3) of the GDPR should also be fully incorporated into the agreement and worked through like a checklist. The alternatives applicable to the specific service relationship should be ticked. Blank fields should be filled in, if necessary, according to the specific contract. Remuneration and liability regulations for the individual services of the contractor should be agreed in the main contract.

1. Subject matter and duration of the contract

(1) Subject

✓ The subject matter of the contract results from the framework agreement on the provision of a complete mobility solution (hereinafter service agreement).

or

⬜ The subject of the data handling contract is the performance of the following tasks by the contractor: ………………………………………………………………….. (description of the tasks)

(2) Duration

✓ The duration of this contract (term) corresponds to the term of the performance agreement.

or (especially if there is no performance agreement on duration)

☐ The contract includes a one-time execution.

or

☐ The duration of this contract (term) is limited until the ....

or

☐ The contract is concluded for an indefinite period of time and can be ....terminated by either party with a notice period of ....at. The possibility of termination without notice remains unaffected.

(3) The contract shall apply without prejudice to the preceding paragraph for as long as the Contractor processes personal data of the Client (including backups).

(4) Insofar as other agreements between the Client and the Contractor result in other arrangements for the protection of personal data, this contract for commissioned processing shall take precedence, unless the parties expressly agree otherwise.

2. Concretisation of the content of the contract

(1) Nature and purpose of the intended processing of data

☐ The type and purpose of the processing of personal data by the contractor for the client are ....specifically described in the service agreement dated

or

☐ Detailed description of the subject matter of the contract with regard to the nature and purpose of the Contractor's tasks: ....

(2) Type of data

☐ The type of personal data used is specifically described in the service agreement under: ....

or

✓ The following types/categories of data are the subject of the processing of personal data (enumeration/description of the categories of data)

- ✓ Personal master data
- ✓ Communication data (e.g. telephone, e-mail)
- ✓ Contract master data (contractual relationship, product or contractual interest)
- ✓ Customer history
- ✓ Contract billing and payment data
- ☐ Planning and control data
- ☐ Information (from third parties, e.g. credit agencies or public directories)
- ✓ Driving licence data

(3) Categories of persons concerned

☐ The categories of data subjects concerned by the processing are specifically described in the performance agreement under: ....

or

✓ The categories of data subjects affected by the processing include:

  ✓ Customers

  □ Interested parties

  ✓ Subscribers

  ✓ Employees

  □ Suppliers

  □ Sales representative

  □ Contact

  □ ...

3. Technical-organisational measures

(1) The Contractor shall take all necessary technical and organisational measures in its area of responsibility in accordance with Art. 32 of the GDPR to protect personal data and shall provide the Client with the documentation for review [Annex 1]. If accepted by the Client, the documented measures shall become the basis of the contract.

(2) Insofar as the review/audit of the Client reveals a need for adjustment, this shall be implemented by mutual agreement.

(3) The agreed technical and organisational measures are subject to technical progress and further development. In this respect, the contractor shall be permitted to implement alternative adequate measures in the future. In doing so, the security level of the specified measures may not be undercut. The Client shall be informed immediately of any significant changes which are to be documented by the Contractor.

4. Rights of data subjects

(1) The contractor shall support the principal within his area of responsibility and as far as possible by means of suitable technical and organisational measures in responding to and implementing requests from data subjects regarding their data protection rights. The Contractor may not inform, port, correct, delete or restrict the processing of data processed on behalf of the Client on its own authority, but only in accordance with the Client's documented instructions. If a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.

(2) Insofar as included in the scope of services, the rights to information, correction, restriction of processing, deletion and data portability shall be ensured directly by the contractor in accordance with documented instructions from the client.

5. Quality assurance and other obligations of the contractor

(1) In addition to compliance with the provisions of this Agreement, the Contractor shall have its own statutory obligations pursuant to the GDPR; in this respect, it shall in particular ensure compliance with the following requirements:

a) Maintaining confidentiality in accordance with Art. 28 (3) sentence 2 lit. b, 29, 32 (4) DS-GVO. When carrying out the work, the contractor shall only use employees who have been obligated to maintain confidentiality and who have previously been familiarised with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who legitimately has access to personal data may process this data exclusively in accordance with the Client's instructions, including the powers granted in this contract, unless they are legally obliged to process it.

b) The contracting authority and the contractor shall cooperate with the supervisory authority in the performance of its duties upon request.

c) The immediate information of the Client about control actions and measures of the supervisory authority, insofar as they relate to this contract. This shall also apply to the extent that a competent authority investigates the Contractor in the context of administrative offence or criminal proceedings with regard to the processing of personal data in the course of commissioned processing.

d) Insofar as the Client, for its part, is subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party, another claim or a request for information in connection with the commissioned processing at the Contractor, the Contractor shall support it to the best of its ability.

e) The contractor shall regularly monitor the internal processes as well as the technical and organisational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

f) Verifiability of the technical and organisational measures taken vis-à-vis the Client within the scope of its control powers pursuant to clause 8 of this contract.

g) The Contractor shall immediately report breaches of the protection of personal data to the Client in such a way that the Client can fulfil its legal obligations, in particular pursuant to Articles 33 and 34 of the GDPR. The contractor shall prepare documentation of the entire process and make it available to the client for further measures.

h) The Contractor shall support the Client in its area of responsibility and as far as possible within the scope of existing information obligations vis-à-vis supervisory authorities and data subjects and shall provide it with all relevant information in this context without delay.

i) Insofar as the Client is obliged to carry out a data protection impact assessment, the Contractor shall support the Client taking into account the type of processing and the information available to it. The same applies to any existing obligation to consult the competent data protection supervisory authority.

(2) This contract does not release the contractor from compliance with other requirements of the GDPR.

6. Subcontracting relationships

(1) Subcontracting relationships within the meaning of this regulation shall be understood to be those services which directly relate to the provision of the main service. This does not include ancillary services used by the contractor, e.g. telecommunications services, postal/transport services, cleaning services or guarding services. Maintenance and testing services shall constitute a subcontracting relationship if they are provided for IT systems which are provided in connection with a service of the contractor under this contract. However, the Contractor shall be obliged to enter into appropriate and legally compliant contractual agreements and to take control measures to ensure data protection and data security of the Client's data also in the case of outsourced ancillary services.

(2) The Contractor may only engage subcontractors (further processors) with the prior express written or documented consent of the Client.

a) ☐ Subcontracting is not permitted.

b) ✓ The Client consents to the commissioning of the subcontractors designated in Annex 2 subject to the condition of a contractual agreement with the subcontractor in accordance with Article 28 (2-4) of the GDPR.

The contractual agreement shall be presented to the client at the client's request, with the exception of business clauses not related to data protection law.

c) ☐ The outsourcing to subcontractors or

☐ the change of the subcontractor existing in accordance with Annex 2 are permitted insofar as:

- the Contractor gives the Client prior written or textual notice of such outsourcing to subcontractors within a reasonable time, which shall not be less than 14 days; and
- the Client does not object to the planned outsourcing in writing or in text form to the Contractor by the time the data is handed over, and
- a contractual agreement in accordance with Article 28 (2-4) of the GDPR is used as a basis.

(3) The transfer of the Client's personal data to the subcontractor and the subcontractor's initial activity shall only be permitted once all requirements for subcontracting have been met. Compliance with and implementation of the technical and organisational measures at the subcontractor shall be checked by the contractor in advance of the processing of personal data, taking into account the risk at the subcontractor, and then regularly. The contractor shall make the control results available to the client upon request. The Contractor shall also ensure that the Client can exercise its rights under this Agreement (in particular its control rights) directly against the subcontractors.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the contractor shall ensure that it is permissible under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be used.

(5) A further outsourcing by the subcontractor

☐ is not permitted;

✓ requires the express consent of the principal (at least in text form);

☐ requires the express consent of the main contractor (at least in text form).

All contractual provisions in the contractual chain shall also be imposed on the further subcontractor.

7. International data transfers

(1) Any transfer of personal data to a third country or to an international organisation shall require documented instructions from the principal and shall be subject to compliance with the requirements for the transfer of personal data to third countries under Chapter V of the GDPR.

☐ The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area.

- ✓ The contracting authority permits a data transfer to a third country. Annex 2 specifies the measures to ensure an adequate level of protection from Art. 44 et seq. DS-GVO are specified in the context of subcontracting.

(2) Insofar as the Client instructs a data transfer to third parties in a third country, the Client shall be responsible for compliance with Chapter V of the GDPR.

8. Control rights of the principal

(1) The Client shall have the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be named in individual cases. It shall have the right to satisfy itself of the Contractor's compliance with this Agreement in its business operations during normal business hours by means of spot checks, which must generally be notified in good time.

(2) The Contractor shall ensure that the Client can satisfy itself of the Contractor's compliance with its obligations under Article 28 of the GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

(3) Evidence of the technical-organisational measures for compliance with the special requirements of data protection in general as well as those relating to the contract can be provided through

- ✓ compliance with approved rules of conduct in accordance with Art. 40 DS-GVO;
- □ certification in accordance with an approved certification procedure pursuant to Art. 42 DS-GVO;
- ✓ current attestations, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors);
- ✓ suitable certification through IT security or data protection audit (e.g. according to BSI-Grundschutz).

9. Authority of the principal to issue instructions

(1) The Contractor shall process personal data only on the basis of documented instructions from the Client, unless it is obliged to process such data under the law of the Member State or under Union law. The Client shall confirm verbal instructions without delay (at least in text form). The Client's initial instructions shall be determined by this contract.

(2) The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend

the implementation of the corresponding instruction until it is confirmed or amended by the Client.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall not be made without the knowledge of the client. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data required with regard to compliance with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the Client - but at the latest upon termination of the service agreement - the Contractor shall hand over to the Client or, after prior consent, destroy in accordance with data protection law all documents, processing and utilisation results produced and data files connected with the contractual relationship that have come into its possession. The same applies to test and reject material. The protocol of the deletion shall be submitted upon request.

Roskilde , 12.01.2024

Leos Jensen

Client (Customer)

Aachen, 12.01.2023

Michael Minis

Contractor (Digital Mobility Solutions GmbH)

Annex 1 - Technical-organizational measures

Measures to ensure confidentiality and integrity, as well as availability (at the offices of DMS GmbH)

2.1	**Access control measures to server rooms and offices**
2.1.1	Is user personal data stored on servers that you operate locally? yes ☐ no ☒
2.1.1.1	DMS GmbH does not have its own server. Locations of the servers / server room / data center used are: **Location 1**: Amazon Web Services LLC, Frankfurt **Location 2**: Host Europe, Germany
2.1.2	Location of workstations from which personal data is accessed: Workstations of employees
2.1.3	Access to the offices is partially video-monitored by Deutsche Bahn
2.1.4	Access to the building via system locking system. Are there key and lock regulations? yes ☒ no ☐
2.1.5	Access rights are assigned on a personalized basis by means of key allocation. Employees with keys for the system locking system have access to the offices. ☒ Employees without a key for the system locking system, accompanied by employees with a key for the system locking system ☒ Visitors, accompanied by employees with keys for the system locking device ☒ Cleaning service, accompanied by employees with keys for the system locking device
2.2	**Access control measures**
2.2.1	Defined process for (largely centralized) assignment of user IDs and access authorizations when new employees are hired and when employees leave the company or in the event of organizational changes.
2.2.2	User profiles are created by the technical management.
2.2.3	User permissions are managed by the technical management.
2.2.4	Screens are locked when the user is inactive, after 10 minutes
2.2.5	Passwords are created according to the guidelines for secure passwords
2.2.6	The following measures are taken in case of loss, forgetting or spying of a password: ☒ Admin assigns new initial password ☒ Passwords for other systems are renewed, unless covered by central access
2.2.7	Authentication for remote access is performed by Authentication with ☒ User name ☒ Password ☒ 2 Factor Authorization ☒ via VPN
2.2.8	The systems are protected by a firewallThis is updated regularly: ☒ yes ☐ noIt is administered by ☒ own IT ☐ external service provider
2.2.9	Data carriers are encrypted
2.3	**Access control measures**
2.3.1	Data is removed according to the guidelines for secure destruction / deletion :☒ Shredders are available for paper waste ☒ Data carriers (USB sticks, hard disks) are physically destroyed by your own IT
2.3.2	The Clean Desk Policy applies to the office premises and workplaces

2.3.3	Access to data is regulated by the authorization concept and managed by a few administrators
2.4	**Separation control measures**
	Data collected for different purposes are processed separately, logically and physically :☒ Separation of the productive, development, and test environments☒ Access through authorization concept and definition of database rights
2.5	**Measures for pseudonymization**
2.5.1	Separation of assignment data and storage in separate secured system in compliance with legal retention periods
2.6	**Disclosure control measures**
2.6.1	The transfer of personal data is encrypted throughout, using☒ SSH or VPN. ☒ HTTPS (TLS 1.2) ☒ Signature procedure
2.6.2	Keys and certificates are managed by the company's own IT.
2.6.3	The data transfer and deletion deadlines are detailed in paragraphs 6 and 7 and in Appendix 3.
2.6.4	Data is passed on anonymized or pseudonymized.
2.7	**Input control measures**
2.7.1	The entry, modification and deletion of data is technically logged.
2.7.2	Entries, changes and deletion of data by individual user names (not user groups) is clearly traceable. (see authorization concept)
2.8	**Availability control measures**
2.8.1	There is a backup and recovery concept, ☒ functionality is regularly tested☒ data recovery is regularly tested and logged☒ backups are stored on a second redundant server (in a different location from the first)☒ backups are encrypted☒ there are separate partitions for operating systems and data
2.9	**Incident Response Management**
2.9.1	Security breaches and data protection incidents are responded to in accordance with a fixed concept :☒ Notification of security incident / data pass (also with regard to notification obligations to supervisory authorities) ☒ Documentation of all details via ticket system☒ Formal process for postprocessing

2.10	**Privacy-friendly default settings according to Art. 25 DSGVO**
2.10.1	The settings are configured in a privacy-friendly way (Privacy by Default)

Annex 2 - Approved subcontracting relationships

Please find the list of subcontractors in this folder.

full link:

https://drive.google.com/drive/folders/17QSCmVP7EwCZBhDnQ7KxdzyW5HsC5nN1?usp=share_link

Annex 3: Measures to be taken in the event of a request for deletion at DMS GmbH

Process description

User wants to **delete** his **user account**

1. The platform checks if the **conditions for deleting the account are fulfilled** (last booking must be 3 months ago - this ensures that no traffic offenses are open and the chargeback deadlines for SEPA are over, there must be no more open conflicts and receivables.
2. If the conditions are not met, the user cannot close his account.
3. If the conditions are met, the user can close his account and at the same time receive the possibility to express a **deletion request according to the GDPR.**
4. The deletion of the account triggers a confirmation email with further information to the user. At the same time, a system incident is created and an email with all important information and high priority is sent to Customer Support and to the provider(s) informing about the deletion of the user.
5. If the user also chooses the deletion request according to the GDPR, a system incident will be created and an email with all important information and high priority will be sent to Customer Support and to the provider(s) informing about the user's deletion request according to the GDPR.
6. If the Provider issues the order to delete the User's personal data, a manual process is initiated in which all data from-
   Portal-
   Prerelease-
   Stripe (bank details)-
   any third-party providers (e.g. CleverReach newsletter)
   - contact lists (Drive), service phone, service cell phone, etc. are
   deleted. Anonymization or pseudonymization is only permissible in coordination with the client and only if deletion is not technically feasible.
7. Customer Support sends a confirmation email to the data subject that his or her personal data has been deleted, and this email is also eliminated.