Data Processing Agreement

between

Carly Solutions GmbH & Co. KG, with its registered office at Kolpingring 8, 82041 Oberhaching, Germany ("Processor")

and

[Customer name to be included], with its registered office at **[insert address]** ("Controller")

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (hereinafter referred to as "Clauses" or "Data Processing Agreement") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 ("GDPR") and the otherwise applicable data protection laws.

(b) The Controllers and Processors listed in Appendix I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) GDPR and the otherwise applicable data protection laws.

(c) These Clauses apply to the processing of personal data as specified in Appendix II.

(d) Appendices I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the Controller is subject under the applicable data protection laws, in particular the GDPR.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V GDPR or the otherwise applicable data protection laws.

(g) These Clauses apply to the processing activities carried out by the Processor on behalf of the Controller under the [contract] concluded between the Parties (hereinafter also referred to as the "Agreement"), as specified in more detail in Appendix II. The Clauses apply accordingly in case

the Processor acts as a sub-processor and the Controller as a processor of its customers.

Clause 1A

Demarcation of Processing on Behalf of the Controller and Processing for Own Purposes

(a) These Clauses (Data Processing Agreement) govern exclusively the processing of personal data carried out by the Processor on behalf and on documented instructions of the Controller for the Controller's purposes in accordance with Article 28 GDPR.

(b) Processing of personal data carried out by the Processor for its own purposes is not subject to these Clauses. This includes, in particular, the processing of Vehicle Data and personal data contained therein by the Processor for its own business purposes as described in [Section 12.4 of the Provider's General Terms and Conditions], including (i) quality assurance, diagnostic validation, and systematic further development of the Processor's products and services (including the training and optimization of algorithms and AI models), and (ii) the analysis, aggregation, and enrichment of data to create products (e.g., evaluation models, scores, forecasts) that the Processor may distribute to third parties.

(c) For the processing of personal data for its own purposes referred to in paragraph (b), the Processor acts as an independent controller separate from the Controller within the meaning of Article 4(7) GDPR. The Processor relies on its own legal basis pursuant to Article 6 GDPR for such processing, in particular legitimate interests pursuant to Article 6(1)(f) GDPR or, where applicable, consent obtained by the Controller. The Processor bears sole responsibility under data protection law for such processing and is independently obliged to comply with all requirements of applicable data protection laws, in particular the GDPR.

(d) The provisions of these Clauses, in particular the Controller's right to issue instructions, the Processor's obligations regarding security, documentation, sub-processing, and assistance to the Controller, as well as the liability provisions, shall not apply to the processing of personal data for the Processor's own purposes pursuant to paragraph (b).

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Appendices or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in the GDPR or in the otherwise applicable data protection laws respectively, those terms shall have the same meaning as in the relevant data protection law.

(b) These Clauses shall be read and interpreted in the light of the provisions of the GDPR and the otherwise applicable data protection laws.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in the applicable data protection laws, in particular the GDPR, or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a Controller or a Processor by completing the Appendices and signing Appendix I.

(b) Once the Appendices in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a Controller or a Processor, in accordance with its designation in Appendix I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in Appendix II.

Clause 7

Obligations of the Parties

7.1. Instructions

(a) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe the GDPR or any other applicable data protection laws.

(c) Instructions that go beyond the provisions of the Agreement and are not necessary to prevent or remedy legal violations within the scope of responsibility of the Processor shall only be carried out if the Processor agrees to them. The Processor may demand reasonable reimbursement of costs for carrying out these instructions.

7.2. Purpose limitation

The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Appendix II, unless it receives further instructions from the Controller.

7.3. Duration of the processing of personal data

Processing by the Processor shall only take place for the duration specified in Appendix II.

7.4. Security of processing

(a) The Processor shall at least implement the technical and organisational measures specified in Appendix III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (sensitive data), the Processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with these Clauses.

(c) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly the GDPR and otherwise applicable data protection laws. At the Controller's request, the Processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Processor.

(d) The Controller may choose to conduct the audit by itself or mandate an independent auditor, in which case the Controller's own costs and the costs of engaging an independent auditor shall be borne solely by the Controller. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice.

(e) Provided that the Processor informs the Controller of the costs incurred prior to conducting the audit or providing the information, the Processor may charge the Controller for the reasonable costs (including the costs of internal staff and external service providers) incurred in connection with responding to information requests and assisting with audits.

(f) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The Processor has the Controller's general authorisation for the engagement of sub-processors from an agreed list. The Processor shall specifically inform in writing the Controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object.

(b) Where the Processor engages a sub-processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data Processor in

accordance with these Clauses. The Processor shall ensure that the sub-processor complies with the obligations to which the Processor is subject pursuant to these Clauses and to the applicable data protection laws, in particular the GDPR.

(c) At the Controller's request, the Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including personal data, the Processor may redact the text of the agreement prior to sharing the copy.

(d) The Processor shall remain fully responsible to the Controller for the performance of the sub-processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the sub-processor to fulfil its contractual obligations.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the Processor shall be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under Union or Member State law or the otherwise applicable law to which the Processor is subject and shall take place in compliance with Chapter V GDPR or the otherwise applicable data protection laws.

(b) The Controller agrees that where the Processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V GDPR or otherwise applicable data protection laws, the Processor and the sub-processor can ensure compliance with Chapter V GDPR or the otherwise applicable data protection laws by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) GDPR or by providing other transfer safeguards in accordance with the otherwise applicable data protection laws, provided the conditions for the use of those standard contractual clauses or transfer safeguards are met.

Clause 8

Assistance to the Controller

(a) The Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the Controller.

(b) The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the Processor shall comply with the Controller's instructions

(c) In addition to the Processor's obligation to assist the Controller pursuant to Clause 8(b), the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment) where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a Data Protection Impact Assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 GDPR.

(d) The Processor may require the Controller to reimburse it for the costs (including internal costs) associated with the assistance referred to in Clause 8(b) and (c).

(e) The Parties shall set out in Appendix III the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations under Articles 33 and 34 GDPR or the applicable data protection laws, insofar as these impose an obligation on the Controller to report to the competent supervisory authority or to notify the data subjects in the event of a personal data breach, taking into account the nature of processing and the information available to the Processor.

9.1 Data breach concerning data processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, in particular pursuant to Article 33(3) GDPR or in accordance with the applicable data protection laws, shall be stated in the Controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 GDPR or any such obligation under the applicable data protection laws, with the obligation to communicate without undue delay the personal data breach to the data subject, when the

personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the Processor

In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

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

(2) the details of a contact point where more information concerning the personal data breach can be obtained;

(3) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of the GDPR and otherwise applicable data protection laws, 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.

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

(1) 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;

(2) the Processor is in substantial or persistent breach of these Clauses or its obligations under applicable data protection laws, in particular the GDPR;

(3) the Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to the applicable data protection laws, in particular the GDPR.

(c) 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.

(d) Following termination of the contract, the Processor shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or, return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is

deleted or returned, the Processor shall continue to ensure compliance with these Clauses.

Clause 11

Liability and Indemnification

The Processor's liability arising from or in connection with this Data Processing Agreement, whether in contract or tort, is subject to [Section 9 (Liability) of the Provider's General Terms and Conditions]. The provisions on liability in [Section 9 of the Provider's General Terms and Conditions]shall apply notwithstanding the provisions of this Data Processing Agreement and shall take precedence in the event of a conflict with the provisions of this Data Processing Agreement.

Clause 12

Transfer of personal data to the Controller

(a) In order for the Processor to provide the services under the Agreement, it is necessary to transfer personal data from the European Economic Area ("EEA") to the Controller, who is located outside the EEA in the USA.

(b) For the purposes of the data transfer referred to in a), the Parties agree to be bound by the EU Standard Contractual Clauses (Module 4: Processor to Controller transfers). The EU Standard Contractual Clauses (Module 4: Processor to Controller transfers) in Appendix IV shall therefore form part of this Data Processing Agreement.

Clause 13

Changes, invalidity, applicable law, and place of jurisdiction

(a) All amendments and additions to this Data Processing Agreement must be made in text form. This also applies to the amendment of this text form clause. Section 305b German Civil Code (BGB) remains unaffected. Notices of termination must be made in writing. Declarations that must be made in writing may also be made by email. The receipt of the declaration shall be decisive for compliance with the deadlines specified in this agreement, unless expressly stipulated otherwise.

(b) Should certain provisions of this Data Processing Agreement be or become invalid in whole or in part, this shall not affect the validity of the remaining provisions. In this case, the Parties undertake to replace the invalid

provision with a valid provision that comes as close as possible to the economic purpose of the invalid provision. The same applies to any gaps in this agreement.

(c) The law of the Federal Republic of Germany shall apply.

(d) The exclusive place of jurisdiction for all legal disputes arising from or in connection with this Data Processing Agreement is the district of the Regional Court of Munich I (Landgericht München I).

APPENDIX I

LIST OF PARTIES

Controller(s): [*Identity and contact details of the Controller(s), and, where applicable, of the Controller's data protection officer]*

1. Name: … *[JD Comment: To be included.]*

Address: … *[JD Comment: To be included.]*

Contact person's name, position and contact details: … *[JD Comment: To be included.]*

Signature and accession date: … *[JD Comment: To be signed.]*

Processor(s): [*Identity and contact details of the Processor(s) and, where applicable, of the Processor's data protection officer]*

1. Name: Carly Solutions GmbH & Co. KG

Address: Kolpingring 8, 82041 Oberhaching, Germany

Contact person's name, position and contact details: Robert Prosciak, Head of Operations, robert@mycarly.com, +491622632852

Signature and accession date: … *[JD Comment: To be signed.]*

APPENDIX II

DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

- Employees of the Controller
- Potential and actual customers of the Controller

Categories of personal data processed

- User name
- User email address
- Report ID
- License plate
- Vehicle Identification Number (VIN)
- Mileage
- Error codes
- Battery state of health
- Crash data

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

Nature of the processing

The nature of the processing is further described by the purposes of the data transfer and further processing set out below.

Purpose(s) for which the personal data is processed on behalf of the Controller

As set forth in the Agreement concluded between Controller and Processor.

Duration of the processing

The duration of the processing is subject to the term and termination of the Agreement.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

N/A

APPENDIX III

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Measures for pseudonymization and encryption of personal data

- **Encryption:** Use of AES-256 or RSA encryption techniques for data encryption both during transmission (Transport Layer Security - TLS) and storage (Data at Rest Encryption).

Measures to continuously ensure the confidentiality, integrity, availability, and resilience of systems and services related to processing

- **Confidentiality:** Access controls and authorization management to ensure that only authorized persons have access to personal data.
- **Availability:** Implementation of high-availability systems, redundancy, and load balancing to minimize downtime.
- **Resilience:** Regular stress testing and performance monitoring to verify and ensure the resilience of the systems.

Measures to ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident

- **Backups:** Regular automatic backups that are stored securely and encrypted in geographically distributed locations.

Procedures for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing

- **Security audits:** Regular internal and external audits to verify compliance with security policies and standards.

Measures for identifying and authorizing users

- **Authentication:** Use of multi-factor authentication (MFA) to verify the identity of users.
- **Authorization:** Implementation of a role-based access control (RBAC) system to ensure that users only have access to data that is necessary for their tasks.

Measures to protect data during transmission

- **Encryption:** Use of TLS (Transport Layer Security) to encrypt data during transmission between systems and networks.

- **VPN:** Use of virtual private networks (VPN) for secure connections to internal networks.

Measures to protect data during storage

1. **Encryption:** Use of strong encryption methods (e.g., AES-256) to secure data at rest.
2. **Access controls:** Implementation of strict access controls and logging of access events.

Measures for internal governance and management of IT and IT security

- **Training:** Regular training and awareness measures for employees to promote security awareness.

Measures to ensure data minimization

- **Data minimization:** Implementation of processes to ensure data minimization by collecting and processing only the most necessary data.
- **Data deletion:** Regular review and secure deletion of data that is no longer needed in accordance with defined retention policies.

Measures to ensure data quality

- **Data quality:** Establishment of mechanisms to ensure data quality through regular reviews, cleanups, and updates.

Validation: Use of validation tools and procedures to ensure the accuracy and completeness of the data collected.

Appendix IV

EU Standard Contractual Clauses (Module 4: Transfer Processor-to-Controller)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

1 Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2) (c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) N/A

(iv) N/A

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organizational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data ([2]), the nature,

2 This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex

scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point

life or sexual orientation, or data relating to criminal convictions or offences.

authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

N/A

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

(Not applicable, as the Processor established in the EU does not combine the personal data received from the Controller established in the third country with personal data collected by the Processor in the EU.)

Clause 15

Obligations of the data importer in case of access by public authorities

(Not applicable, as the Processor established in the EU does not combine the personal data received from the Controller established in the third country with personal data collected by the Processor in the EU.)

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the Federal Republic of Germany.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of the Federal Republic of Germany.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

Annex I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: Carly Solutions GmbH & Co. KG

Address: Kolpingring 8, 82041 Oberhaching, Germany

Contact person's name, position and contact details: Robert Prosciak, Head of Operations, robert@mycarly.com, +491622632852

Activities relevant to the data transferred under these Clauses: As set forth in Annex I.B.

Signature and date: … *[JD Comment: To be signed.]*

Role: Processor

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: … *[JD Comment: To be included.]*

Address: … *[JD Comment: To be included.]*

Contact person's name, position and contact details: … *[JD Comment: To be included.]*

Activities relevant to the data transferred under these Clauses: As set forth in Annex I.B.

Signature and date: … *[JD Comment: To be signed.]*

Role: Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Employees of the Controller
- Potential and actual customers of the Controller

Categories of personal data transferred

- User name
- User email address
- Report ID
- License plate
- Vehicle Identification Number (VIN)
- Mileage
- Error codes
- Battery state of health
- Crash data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal data is transferred on an ongoing basis.

Nature of the processing

The nature of the processing is further described by the purposes of the data transfer and further processing set out below.

Purpose(s) of the data transfer and further processing

As set forth in the Agreement concluded between data exporter and data importer.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The data exporter processes personal data for as long as necessary for the purposes of the data transfer and further processing described above, and in accordance with applicable laws regarding retention periods.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

N/A

* * *