Commissioned Processing Contract

between

. . . . . .Customer number

. . . . . .Company name

. . . . . Street/ no.

. . . . . .Post code, city

. . . . . Country

− hereinafter referred to as the Principal –

and

HELLA Gutmann Solutions GmbH
Am Krebsbach 2
79241 Ihringen
Germany

− hereinafter referred to as the Agent –

- The Agent and the Principal together are hereinafter referred to as the Parties or individually as the Party.

WHEREAS the Agent develops and markets a service solution which should enable garages to organize service orders transparently at all levels and accelerate them. In addition to the provision of digital inspection plans, manuals and data important for the service regarding the vehicle in question at several work stations, work should be documented and after the completion of a service order optionally also entered into the vehicle manufacturers' portals. In order to perform these tasks, the Agent receives data from the Principal's company about the vehicle and the customer via an electronic interface. This data also includes data which constitutes personal data pursuant to the General Data Protection Regulation ("GDPR"), e.g. the licence plate number and the vehicle identification number.

NOW THEREFORE, in order to control how said data is handled, the Parties herewith enter into the following contract.

1. Subject matter, scope and duration of the processing

1.1. The Principal commissions the Agent with the processing and use of the data described under 1.2. while observing the rights and obligations laid down in this contract.

1.2. The data covered by this contract is personal data, which the Agent is sent in connection with the repair/servicing of vehicles from the Principal's business, i.e. details about the customers of the Principal, the vehicle identification numbers (FIN/VIN) and official licence plate numbers. This data shall hereinafter be referred to as "Contractual Data".

1.3. According to the current state of affairs the Contractual Data currently includes the following type of data:

- Name, address, telephone number of the customer and the customer's order number in the garage
- VIN/FIN chassis number, vehicle licence plate number

1.4. The Agent records, saves and processes the Contractual Data. This processing of the Contractual Data including the transfer through OE Service GmbH to the respective vehicle manufacturer shall be done solely to complete the performance from the service agreement and thus the fulfilment of the Agreement.

1.5. The Agent shall save the Contractual Data until the end of the contractual relationship (figure 12.) or until it has been instructed to delete said data at an earlier date by the Principal. If so required by statutory regulations, it shall be permissible for the data to be saved for a period in excess of the above.

1.6. The following persons are affected by the said transfer and processing of the Contractual Data:

- Customers of the Principal (including consumers),
- Vehicle owners,
- Employees of the Principal.

2. Technical and organisational measures for data privacy

2.1. The Agent undertakes to effectively protect the Contractual Data according to the state of the art from unauthorised access, change, destruction or loss, unauthorised transfer, any other unauthorised processing and other misuse and to take all technical and organisational measures ("TOMs") required in accordance with article 32 GDPR. The TOMs should ensure that the Contractual Data is secured to the degree necessary as well protected against misuse, loss and unauthorised access by third parties.

2.2. The current status of the TOMs initiated by the Agent is outlined in Annex 1. As long as the implementation costs are in an appropriate ratio to the risk for the rights and liberties of the persons affected, the Agent shall adjust its TOMs in the course of the contractual relationship if the measures taken no longer correspond to the current state of the art and/or adjustments are necessary due to organisational developments. The security level of the TOMs outlined in Annex 1 may not be undercut as a result. The Agent shall document any changes to the TOMs.

2.3. In the event of cases stated in figures 6.3. and 6.4. (data breaches), the Agent shall adapt its TOMS subject to figure 2.2. of this contract, if this is suitable and necessary for the future avoidance of such breaches. The parties shall additionally take suitable measures to minimise any negative consequences for those affected.

3. Rights and obligations of the Principal, control measures

3.1. Solely the Principal shall be responsible for assessing if the processing is permissible pursuant to article 6 para. 1 GDPR as well as for upholding the rights of the persons affected in accordance with article 12 to 22 GDPR.

3.2. The Principal shall be entitled to convince itself that the Agent is upholding the Toms concluded in accordance with figure 2 of this contract, through inspections on site, as well as according to the proviso of figure 3.3 before the start of the data processing and then regularly at reasonable intervals after agreeing an appointment. The Principal shall not be entitled to carry out the inspection itself. Instead it must contract experts for the inspection who must assure the Agent that they shall only inspect the compliance with obligations outlined in article 28 GDPR and only convey these results to the Principal, thus in particular shall not divulge any of the Agent's company secrets to the Principal.

3.3. The Principal shall furthermore be entitled to demand from the Agent details and information about the implementation of the TOMs in accordance with figure 2 as well as about the upholding of all other obligations specified in article. 28 GDPR. The Agent can comply with such a demand itself or through a third party, for example by:

3.3.1. Providing information itself about the implementation of the TOMs;

3.3.2. Submitting a certificate, a report or an excerpt of a report by an independent third party (e.g. an expert).

3.4. The Principal must bear any costs which may be incurred in the scope of the inspections in accordance with figures 3.2 to 3.3. of this contract, especially by contracting a third party, if the Principal contracted the third party itself or demands that the Agent appoints the third party.

3.5. The Principal shall inform the Agent without delay if it ascertains any faults or irregularities when inspecting the TOMs.

4. Rights and duties of the Agent

4.1. The Agent as well as anyone under its authority, who has access to the Contractual Data, shall solely process the Contractual Data on behalf of the Principal according to its instructions and in the scope of the purpose of this contract unless it is obligated to a different processing due to the law of the European Union or of the member states which the Party is subject to. In such a case the Agent shall notify the Principal of these legal requirements before the processing, unless the law in question prohibits such notification due to an important public interest.

4.2. Outside the instructions of the Princ ipal, the Agent may neither collect, process or use the Contractual Data for its own purpose nor for the purpose of third parties.

4.3. The Agent may only correct, delete or block the Contractual Data if instructed to do so by the Principal, unless there are justified interests of the Agent which oppose this.

4.4. The Agent may not make any copies or duplicates of the Contractual Data without prior authorisation by the Principal. This shall not apply to back-up copies, if they are necessary to ensure a correct data processing, as well as to data which is necessary with regard to upholding statutory archiving obligations.

4.5. The Agent undertakes to pass on to the Principal without delay all enquiries from third parties regarding the Contractual Data. Without written authorisation from the Principal it shall not be entitled to give affected parties or other third parties any information about the Contractual Data.

4.6. If the Agent is granted the possibility of accessing the data processing systems of the Principal, it may only use this access to fulfil its obligations under this contract.

4.7. In view of the type of processing, the Agent shall support the Principal as far as possible with suitable TOMs to meet its obligation to reply to questions regarding rights of the data subject referred to in chapter III of the GDPR. Furthermore it shall, taking into consideration the type of processing and the information it has at its disposal, support the Principal in upholding the obligations outlined in articles 32 to 36 of the GDPR. The Principal must reimburse the Agent for any costs incurred to this end. The Parties have set a rate of €50.00 per hour, if applicable plus VAT.

5. Data protection officer

5.1. Mr Eike Westermann (dataprivacy@hella.com) has been appointed as Data Protection Officer at the Agent.

5.2. The Principal is to be informed without delay if the Data Protection Officer is changed.

6. Notification obligations

6.1. The Agent shall notify the Principal without delay if in its opinion one of the Principal's instructions infringes the GDPR or other data privacy regulations of the European Union or the member states. The Agent may refrain from carrying out the corresponding instruction for so long until the Agent has been informed about the investigation and the results of the investigation of the Principal. If the investigation of the Principal should reveal that there is in fact an infringement against relevant data privacy regulations, the Agent shall not execute the instruction. If after the investigation by the Principal, no consensus can be gained by the Parties about whether the instruction complied with the GDPR or other data privacy regulations of the European Union or the member states, the Parties shall inform the relevant supervisory body and shall obtain their decision in accordance with article 58 Para. 2 a) GDPR.

6.2. If the Agent is aware that the protection of the Contractual Data has been infringed, it must inform the person responsible immediately. The Agent is aware of the infringement of the Contractual Data, if it gains sufficient knowledge to enable it to responsibly report it in accordance with the regulations of the GDPR.

6.3. Fig. 6.2. shall apply accordingly if the Agent is aware of any disruptions to the processing or operating procedure or other infringements of regulations to protect the Contractual Data.

6.4. The Agent must inform the Principal immediately about any checks carried out and measures of the supervisory body if they affect the Contractual Data. This shall also apply if a relevant authority is investigating the Agent. The Agent shall follow any instructions issued by the authorities in connection with the Contractual Data.

7. Managerial authority / scope

7.1. Instructions must be issued in text form (especially in writing or by email).

7.2. The Agent shall document the instructions of the person responsible in a suitable manner.

8. Non-disclosure obligation

8.1. The Agent undertakes to maintain confidentiality during the processing of the Contractual Data.

8.2. The Agent must commit its employees involved in processing the work to maintain confidentiality. Additionally, the Agent must inform these employees about the existing obligation to adhere to the instructions and purpose regarding said data.

8.3. The non-disclosure obligation shall continue also after the contract has terminated.

9. Cross border processing

The contractually agreed data processing shall be performed solely in a member state if the European Union or in another state belonging to the European Economic Area. The data must be stored within the European Union or the European Economic Area. Any processing of the Contractual Data in a third country including data retrieval from such a third country (e.g. by the customer service, help desk etc.), shall require prior written authorisation from the Principal and may only take place if the special conditions of article. 44 and following of the GDPR have been met. The Principal shall grant its consent if the statutory requirements are upheld. This shall also apply to contracting subcontractors in third countries. In order to secure an appropriate data privacy level the Parties undertake to apply standard contractual clauses of the European Commission as soon as these are available. If these clauses have been agreed on by the Agent and the subcontractor, an authorisation from the Principal is no longer required.

10. Subcontractors

10.1. The Agent is entitled to commission subcontractors for the data processing. The contractual agreements with the subcontractor/s must be concluded in such a way that they correspond to the data privacy regulations in the contractual relationship between the Principal and the Agent. A list of the subcontractors currently commissioned is appended to this contract as Annex 2.

10.2. The Agent shall inform the Principal in good time and in advance in text form (especially in writing or by email) about each intended change with regard to the hiring or replacement of subcontractors. The Principal shall be entitled to appeal

against such changes in text form (especially in writing or by email) within two weeks of the receipt of the information.

10.3. The Agent shall ensure that its subcontractor grants it the control rights outlined in figure 3.2. and 3.3. of this contract. With the help of said rights the Agent shall in particular ensure that the subcontractor provides sufficient guarantees that the suitable technical and organisational measures are executed by subcontractor in such a way that the processing is carried out in compliance with the requirements of the GDPR. The results of the investigations are to be documented by the Agent and to be made accessible to the Principal on request.

10.4. Contracts with subcontractors must be laid down in text form (especially in writing or by email).

11. Ownership of data carriers, return of data carriers, deletion

11.1. Any data carriers given to the Principal, on which Contractual Data is stored, are the property of the Principal.

11.2. After completing the contractual work (or earlier if requested to do so by the Principal) the Agent must immediately delete in full the Contractual Data which it has, unless this would involve a breach of any statutory archiving obligations.

11.3. The deletion is to be recorded in writing with a specification of the date and confirmed in text form (especially in writing or by email) to the Principal on its request.

12. Term and termination

12.1. This contract shall come into force on being signed by the Parties and is concluded for an indefinite term.

12.2. The contract can be duly terminated by both Parties with two weeks' notice. This shall not apply if the Agent remains committed under another agreement to process Contractual Data for the Principal. In this case the two weeks' notice period shall only begin once the other agreement has terminated.

12.3. The contract can be terminated by either Party for cause without upholding a notice period. Cause shall exist if, taking all circumstances of the individual case into consideration and assessing the interest of both Parties, the continuation of the contractual relationship until the end agreed or until the end of a period of notice cannot be expected from the Party terminating the contract. This should in particular be the case if a serious violation against the provisions of this contract or against the provisions of the GDPR is committed by the respective other Party.

12.4. Notice of termination must be made in writing as stated in article 126 German Civil Code (BGB).

13. Applicable law / place of jurisdiction / ineffective provisions

13.1. The Parties agree on the application of German law with the exception of the rules on the conflict of laws. The place of jurisdiction for all disputes arising from or in connection with this contract is the headquarters of the Agent.

13.2. If individual provisions of this contract are ineffective or nonexecutable or become ineffective or nonexecutable after signing this contract this shall not affect the effectiveness or executability of the remaining provisions of the contract. The ineffective or nonexecutable provision shall be replaced with an effective or executable one which comes as nearest as possible to the economic aim which the Parties were trying to attain with the ineffective or nonexecutable provision.

Place, Date. . . . . Ihringen, 3 March 2020

. . . .

. . . . . .

Signature the Principal (Managing director)
(Authorised representative 1)

. . . . . Rolf Kunold

Name in capitals

- Annex 1 -

Technical and Organisational Measures

The following technical and organisational measures are to be determined individually and specifically named.

If sensitive data or special types of personal data are covered by the order (e.g. details about trade union membership or health), special protective measures are to be taken. These must be stipulated separately and explained.

The following measures are minimum requirements. They are to be guaranteed at any time by the Agent:

1. Entry checks

Unauthorised persons are forbidden entry (in terms of physical access) to the data processing systems, with which the personal data is processed and used.

Technical and organisational measures for access checks:

- ID card reader, chip card;
- Protective measures against theft, manipulation and damage to the equipment used for the data processing; for example access authorisation concept for the server, UPS and air conditioning in server rooms
- Different security zones on the premises;
- Keeping a log of personnel on site;
- Controlled issue of keys (including access areas);
- Door security system (electrical door openers etc.);
- Factory security, gatekeeper;
- Regulations for entry of external parties;
- Access barriers (e.g. turnstiles);
- Monitoring systems such as alarm systems

2. Physical access checks

Unauthorised persons must be prohibited from accessing the data processing systems.

Technical (code / password protection) and organisational (user master record) measures with regard to the user identification and authentication:

- Authorisation concept and introduction of differentiated access levels (system);
- Individual user IDs;
- Password procedures (i.e. special characters, minimum length, the code is to be changed regularly);
- Process designed and implemented which guarantees that all access rights are revoked immediately if an employee leaves the Agent’s company;
- Firewall;
- Encryption of data carriers in accordance with the acceptable use-policy regulation for the use/disposal of data carriers (e.g. USB, external hard disks);
- Provisions for the access of external parties.

3. Access checks

It must be ensured that to use a data processing system, authorised persons can solely access the data which their access rights entitle them to access, and that personal data cannot be read, copied, changed or deleted without authorisation while said data is being used, processed or stored.

Measures to develop the authorisation concept and the access rights as well as their monitoring and recording:

- An authorisation concept and implementation of differentiated access levels (data);
- All servers are hosted in secure computer centres, which are regularly tested regarding their security;
- It is not possible to install unknown/unauthorised software on the hardware of the Agent;

4. Transfer checks

It must be ensured that during the electronic transfer or during transport or when being saved to a data carrier, the personal data cannot be read, copied, changed or deleted without authorisation.

Measures during the transfer, transport or saving onto data carriers (manually or electronically) as well as during the subsequent inspection:

- Encryption, tunnel connection (VPN = Virtual Private Network);
- Recording of the transfer type / data transferred / recipient transport protection.

5. Input checks

It must be ensured that that it is possible to subsequently check and ascertain if and by whom personal data has been entered into the data processing system or changed or deleted.

Measures to subsequently check, if and by whom the data was entered, changed or deleted:

- Recording system activities (reading, changing, unauthorised access attempts, regular log analysis / special analysis if necessary);
- Regular and systematic evaluation of the logs.

6. Order control

It must be ensured that personal data which is commissioned to be processed is only processed according to the instructions of the Principal.

Measures to demarcate the competences between the Principal and the Agent:

- The employees are separately obliged not to disclose the customer data transferred;
- The customer data has to be treated with at least the same due care as the Agent's own confidential data;
- Steering of the execution of the contract (control / auditing subcontractors by the Agent, the Principal shall receive the results of the self-evaluation of the Agent).

7. Availability check

The Agent must ensure that personal data is protected against co-incidental destruction or loss.

Measures to secure the data (against destruction /loss):

- Back-up procedures;
- Separate storage;
- Mirroring of the hard disks (e.g. RAID);
- Uninterrupted power supply (UPS);
- Concept for the archiving of data;
- Regular control of the status of the system (monitoring);
- Virus protection.

8. Separation checks

It must be ensured that data collected for different purposes can be processed separately.

Measures for the separate processing (saving, changing, deletion and transfer) of data for different purposes:

- Separation of real-time and test system;
- Documented functional separation.

No.	Company	Address	Purpose of the sub-commissioning
1	TecAlliance GmbH	Steinheilstraße 10 85737 Ismaning Germany	For the correct identification of vehicles in Austria, Switzerland, Germany, France and the Netherlands
2	Bisnode Danmsark a/s	Gyngemose Parkvej 50,8 2860 Søborg Denmark	For the correct identification of vehicles in Finland, Norway and Sweden
3	FTZ Autodele & Værktøj A/S	Hvidkærvej 21 5250 Odense SV Denmark	For the correct identification of vehicles in Denmark
4	OE Service GmbH	Dr. Franz-Palla-Gasse 22 9020 Klagenfurt Austria	Data entry and retrieval into and from portal(s) of the vehicle manufacturer
5	Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay Dublin 2 Ireland	Hosting the application