EUROPEAN
COMMISSION

Brussels, XXX
[…](2025) XXX draft

ANNEX

ANNEX

to the

Commission Delegated Regulation

amending Regulation (EU) 2018/858 of the European Parliament and of the Council as regards the standardised access to vehicle on-board diagnostics information and repair and maintenance information, and the requirements and procedures for secure access to on-board diagnostic information

ANNEX

Annex X to Regulation (EU) 2018/858 is amended as follows:

(1) point 1 is replaced by the following:

'1. Introduction

This Annex lays down technical requirements for the access to vehicle OBD information and vehicle repair and maintenance information regardless of the vehicle powertrain type.';

(2) in point 2.1., the second sentence is replaced by the following:

'Compliance with the obligation for manufacturer to provide information about the vehicle OBD system and vehicle repair and maintenance information on their websites through a standardised format shall be presumed by conforming to Part 1 'General information and use case definition', Part 2 'Technical requirements', Part 3 'Functional user interface requirements' of standard EN ISO 18541 – 2021, Part 4 'Conformance test' of standard EN ISO 18541 – 2021 and Part 5 'Heavy duty specific provision' 'Road vehicles – Standardized access to automotive repair and maintenance information (RMI)' of standard EN ISO 18541 – 2018.';

(3) in point 2.5, the introductory wording is replaced by the following:

'2.5. The vehicle repair and maintenance information shall include the following:';

(4) point 2.5.1. is replaced by the following:

'2.5.1. an unequivocal identification of the vehicle and the resulting list of factory-fitted options, as well as of systems, components, separate technical units, parts or equipment for which the manufacturer is responsible;';

(5) point 2.5.4. is replaced by the following:

'2.5.4. information about systems, components, separate technical units, parts, equipment and diagnosis (including minimum and maximum theoretical values for measurements), including information about functions and capabilities necessary for calibration and repair of Advanced Driver Assistance Systems (ADAS), ADS or Driver Control Assistance Systems (DCAS) and related components);';

(6) point 2.5.7. is replaced by the following:

'2.5.7. information required to determine whether a software update or variant coding is necessary for a specific repair and maintenance operation;';

(7) the following point 2.5.7a. is inserted:

'2.5.7a. information required for the identification of the correct software update or variant coding for each system, component, separate technical unit, part or equipment requiring a software update;

By way of exception from point 2.1., if the determination of the correct software version or variant coding requires a backend connection, the manufacturer shall not be required to publish the information required for the identification of the correct software update or variant coding for each system, component, separate technical unit, part or equipment requiring a software update on the website;';

(8) point 2.5.8. is amended as follows:

‘2.5.8. information provided concerning, and delivered by means of, proprietary tools and equipment including the information of any additional tooling, equipment and the user instructions, that are required to carry out a component or system calibration;’;

(9) the following points 2.5.12. and 2.5.13. are added:

‘2.5.12. information provided by the manufacturer to his authorised partners, dealers and repairers or used by the manufacturer for repair and maintenance purposes, necessary for the diagnosis and, where applicable, the repair of traction battery systems as well as its exchangeable units including battery modules ;

2.5.13. vehicle type specific information necessary for the safe handling of parts and components, in particular information necessary for the protection against electric, thermic and chemical hazards from traction batteries; as available to the vehicle manufacturer or its partners.’

(10) point 2.6.2. is replaced by the following:

‘2.6.2. the following information:

a) diagnostic description data referred to in point 3 of appendix 2. The manufacturer shall ensure that this data meets the following requirements:

i) it is made available as electronic directly processable datasets,;

ii) it is of the same level of detail as used by the vehicle manufacturer proprietary diagnostic tools;

iii) it is comprehensively documented;

b) descriptions of necessary off- and onboard interactions needed for the completion of any repair and maintenance job;

The vehicle manufacturer shall make the information referred in point (a) available only for vehicle types for which the type-approval certificate was first granted after 1 September 2020. ’;

(11) the following point 2.6.3. is inserted:

‘2.6.3. information on how to acquire proprietary tools and equipment.’;

(12) the following points 2.6a and 2.6b. are inserted:

‘2.6a. The manufacturer shall make available to manufacturers of repair equipment and generic diagnostic tools all information, technical specification and user instructions for the repair, maintenance and diagnosis of ADAS/ADS/DCAS systems by diagnostic tools.

2.6b. The information referred to in points 2.6. and 2.6a. shall be made available in accordance with the terms and conditions stipulated by the manufacturer in compliance with this Regulation, including payment terms and conditions or use limitations and fees required in accordance with Article 63(1).’;

(13) point 2.9. is replaced by the following:

‘2.9. For the purpose of accessing vehicle OBD information, diagnostics, repair and maintenance, monitoring and inspection, vehicle manufacturer shall enable bi-directional access to the in-vehicle data stream, through all of the following means:

(a) the serial data port on the standardised data link connector referred to in Appendix 1 paragraph 6.5.3 of Annex C5 to UN Regulation No 154 ∗ respectively in accordance with paragraph 4.7.3 of Annex 9B and the reference standard documents set out in Appendix 6 to that Annex to UN Regulation No 49∗∗ ;

(b) any other in-vehicle means of access that is provided by the manufacturer to his authorised partners, dealers and repairers or is used by the manufacturer for repair and maintenance purposes, including Ethernet connectors, non-standardized pins on the standardized OBD port, application programming interfaces used for aftermarket service integration, and wireless local area networks;

(c) any facility that is provided by the manufacturer to his authorized partners, dealers and repairers or is used by the manufacturer to enable remote access to vehicle OBD Information for repair and maintenance, including monitoring and inspection (where monitoring and inspection are performed for repair and maintenance) or remote repair and diagnostics services.

Where the vehicle is in motion, the manufacturer may choose to make the data stream available only for read-only functions.

The manufacturer may implement conditions for accessing the vehicle data stream, to the extent this is necessary and proportionate for compliance with Article 4(5)(d) and Annex II line D4 of Regulation (EU) 2019/2144 and Articles 4(7) 4(8) and Article 6(3) of Regulation (EU) 2024/1257. For access using the means described in 2.9 (a) and (b), such conditions shall not go beyond the conditions that the manufacturer is allowed to apply pursuant to Appendix 4 to this Annex.’

∗ Regulation No 154 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of light duty passenger and commercial vehicles with regards to criteria emissions, emissions of carbon dioxide and fuel consumption and/or the measurement of electric energy consumption and electric range (WLTP) [2021/2039] (OJ L 423, 26.11.2021, pp. 1–603, ELI: https://eur-lex.europa.eu/eli/reg/2021/2039/oj)

∗∗ Regulation No 49 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the measures to be taken against the emission of gaseous and particulate pollutants from compression-ignition engines and positive ignition engines for use in vehicles [2023/64] (OJ L 14, 16.1.2023, pp. 1–473, ELI: https://eur-lex.europa.eu/eli/reg/2023/64/oj)

(14) point 6.1. is replaced by the following:

‘6.1. Compliance with the obligation for manufacturer to provide vehicle repair and maintenance information on their websites through a standardised format shall be presumed by conforming with the Parts of standard ISO 18541-1:2014 to ISO 18541-1:2021, as referred to in point 2.1.

Those requiring the right to duplicate or republish such information shall negotiate directly with the manufacturer concerned. Information for training material shall also be available, and it may be presented through other media than websites.

6.1.1. For the purpose of publishing repair and maintenance information, the manufacturer shall make the information available as files in the format which serves for direct electronic processing of the sets of data contained in those files. The information shall be of the same level of detail as is used by the manufacturer for repair and maintenance purposes. It shall be documented for the purposes of interpretation and updated at the frequency agreed with the independent operator Updates shall be available with the same frequency and timing as they are available to the authorised dealers and repairers. Information shall be offered in packages based on technical information by use case, as available to the manufacturer. The information referred to in the first sentence of this point shall be provided on the basis of terms and conditions stipulated by the manufacturer in compliance with this Regulation, such as payment terms and any compatible conditions or use limitations and the fees required in compliance with Article 63(1) of this Regulation. Information packages defined based on criteria reflecting the information requirements for Use Case 5.1.1., Use Case 5.1.2, Use Case 5.2, Use Case 5.3, Use Case 5.4, Use Case 5.5, Use Case 5.7, Use Case 5.8, Use Case 5.9, Use Case 8 and Use Case 11 of standard ISO 18541-1 2014 shall be presumed compliant.

The manufacturer shall only provide information packages defined based on criteria reflecting the information requirements needed for Use Case 5.3 and Use Case 5.4 in ISO 18541-1:2014 that are only available per vehicle identification number (VIN) where an independent repairer requests so via an Application Programming Interface (API[1]). In such cases, the independent repairer shall transmit a VIN-specific request to the manufacturer through a third party acting on the basis of an agreement with the manufacturer.

Where the information packages are defined based on criteria reflecting the information requirements for Use Case 8 in ISO 18541-1:2014, the manufacturer shall provide to such a third party an API that allows the independent repairer to view and update the electronic maintenance history subject to the additional conditions as specified in the ISO and, where appropriate, manufacturer's conditions and processes for customer agreement. The manufacturer shall do so subject to the same or equivalent processes and required information as those specified in the manufacturer's repair and maintenance information website. In such cases the independent repairer, with the customer's agreement, may transmit a repair or maintenance record update request to the manufacturer through a third party acting on the basis of an agreement with the manufacturer. A certificate compliant with Recommendation ITU-T X.509 of the International Telecommunication Union may be used to verify the identify the independent repairer.

Access to such API may be subject to reasonable fees.

The information shall be structured in a way so that it is later possible to search and filter the information contained in the package by model type classification criteria and other classification criteria used by the vehicle manufacturer own network.

[1] As defined in Article 2 of Commission Implementing Regulation (EU) 2023/138 of 21 December 2022 laying down a list of specific high-value datasets and the arrangements for their publication and re-use

6.1.2. Information on all parts of the vehicle, with which the vehicle, as identified by the VIN and any additional criteria such as wheelbase, engine output, trim level or options, is equipped by the vehicle manufacturer and that can be replaced by spare parts offered by the vehicle manufacturer to its authorised repairers or dealers or third parties by means of reference to original equipment (OE) parts number, shall be made available, in the form of machine readable and electronically processable datasets, in a database that is easily accessible to independent operators.

That database shall comprise the VIN, OE parts numbers, OE naming of the parts, validity attributes (valid-from and valid-to dates), fitting attributes and, where applicable, structuring characteristics.

The information on the database shall be updated regularly. If this information is available to authorised dealers, the updates shall include all modifications to individual vehicles after their production.';

(15) point 6.2.2. is replaced by the following:

'6.2.2. the standard https//ssl-tls (RFC5246) or any successor to this standard shall be used;'

(16) point 6.2.3. is replaced by the following:

'6.2.3. security certificates in accordance with international standard ISO/IEC 9594-8:2020 shall be used for mutual authentication of independent operators and manufacturers;'

(17) point 6.4. is replaced by the following:

'

6.4. Reprogramming of control units, variant coding and activation of replacement parts shall be conducted using non-proprietary hardware, without any dependency on manufacturer hardware in accordance with any of the following:

(a) international standard ISO 22900-2;

(b) SAE J2534-1;

(c) SAE J2534-2;

(d) TMC RP1210B.

Where conducted using Ethernet, reprogramming of control units, variant coding and activation of replacement parts shall be conducted in accordance with either ISO22900-2 or J2534-2.

For the validation of the compatibility of the manufacturer-specific application and the vehicle communication interfaces (VCI), complying with international standard ISO 22900-2 or with SAE J2534-1 or SAE J2534-2 or TMC RP1210B, the manufacturer shall offer either a validation of independently developed VCIs or the information, and loan of any special hardware, required for a VCI manufacturer to conduct such validation .

The manufacturer may charge reasonable and proportionate fees for such validation or information and hardware. Those fees shall not discourage use of such validation or information and hardware.

(18) the following point 6.4a. is inserted:

‘6.4a. As from [OP please insert the date = 6 months after entry into force of this Regulation], the vehicle manufacturer shall make available to independent diagnostic tool manufacturer any of the following software or information for vehicle type for which the type-approval certificate was first granted after 1 September 2020:

(a) software or webservice interfaces to independent diagnostic tool manufacturers for their integration, that enables variant coding, pairing to a vehicle an original replacement part (including software and hardware compatible (as defined by the vehicle manufacturer) remanufactured or re-used part) or a vehicle manufacturer authorized replacement part, as well as the reprogramming of control units with a vehicle's original equipment software according to vehicle manufacturer’s instructions, or;

(b) necessary information, processes and resources necessary to implement variant coding and reprogramming in independent diagnostic tool of the independent diagnostic tool manufacturer.

However, by way of derogation from the time limit specified in the first sentence of this point, the vehicle manufacturer shall make available the software or information referred in points a) and b) above as from the following dates:

(i) [OP, please insert date corresponding to 12 months after entry into force of this Regulation], with regard to vehicles for which the type-approval was first granted after 1 September 2020 but before 6 July 2022;

(ii) [OP, please insert date corresponding to 24 months after entry into force of this Regulation] for any operation involving or dependent on performing software updates.’

(19) the following point 6.4b. is inserted:

‘6.4.b Until the vehicle manufacturer makes available the software or information for vehicle type referred to in point 6.4a and for the period of two years following that date , the use of vehicle manufacturer’s diagnostic hardware and diagnostic software by remote service providers, as referred to in point 1.2. of Appendix 4 , for the purposes of re-programming and variant coding or parts activation shall be subject to the same fees and payment conditions as those applicable to independent repairers, irrespective of whether the diagnostic tools are used remotely.

Furthermore, vehicle manufacturer shall share with any interested diagnostic tool manufacturers, as soon as they are available:

(a) the information necessary for implementing the API between the relevant vehicle manufacturer’s and diagnostic tool manufacturers’ systems,

(1) no later than [OP, please insert date corresponding to 12 months after the entry into force of this Act] for any operation involving or dependent on performing software updates and,

(2) for other operations, no later [OP, please insert date corresponding to than 3 months after the entry into force of this Act] or,

(3) with regard to vehicles for which the type-approval was first granted before 6 July 2022, no later than [OP, please insert date corresponding to 6 months after the entry into force of this Act].

(b) the information necessary for testing the update functionality and interaction for hardware, no later than [OP, please insert date corresponding to 18 months

after the entry into force of this Act] for any operation involving or dependent on performing software updates.';

(20) points 7.2. and 7.3. are deleted;

(21) point 7.4. is replaced by the following:

'7.4. On the basis of a completed certificate on access to vehicle OBD information and vehicle repair and maintenance information, the approval authority may presume that the manufacturer has put in place satisfactory arrangements and procedures with regard to access to vehicle OBD information and vehicle repair and maintenance information, provided that no complaint has been made.';

(22) the following point 7.5. is added:

'7.5. The vehicle OBD information and vehicle repair and maintenance information shall be provided to independent operators at the latest on the date on which the vehicle is placed on the market.';

(23) in Appendix 2, point 3 is replaced by the following:

'3. Information required for the manufacturing of diagnostic tools

In order to facilitate the provision of generic diagnostic tools for multi-make repairers, vehicle manufacturer shall make available the information referred to in points 3.1, 3.2 and 3.3. That information shall include all diagnostic tool functions and all the links to repair information and troubleshooting instructions. The access to the information may be subject to the payment of a reasonable fee.';

(24) Appendix 3 is amended as follows:

(a) in point 2, the following points 2.1.14. and 2.1.15. are added:

'2.1.14. Remote Service Supplier or RSS'

'remote service supplier or RSS' shall mean a service provider performing remotely, as a service provided to the IO in the context of its SERMI related activities, the programming, fitting or activating of parts and equipment on a vehicle.

2.1.15. 'RSS employee'

'RSS employee' shall mean the employee of an approved RSS who, upon authorisation by the CAB, will have access to security-related RMI.';

(b) in point 3, third and fourth point are replaced by the following:

'IOs wishing to receive security-related RMI shall obtain an approval inspection certificate from an accredited CAB.

IO employees who are to handle security-related RMI shall obtain an authorisation inspection certificate from an accredited CAB.';

(c) in point 4.1.1., the following point (f) is added:

'(f) SERMI shall manage a list of sanctioned interpretations, to be used exclusively for the purpose of interpreting the scheme.'

(d) the following point 4.4.2. is added:

‘4.4.2. RSS shall be subject to the responsibilities and requirements laid down in point 4.4.1.’;

(e) the following point 4.5.2. is added:

‘4.5.2. RSS employee shall be subject to the responsibilities and requirements laid down in point 4.5.1.’;

(25) the following Appendix 4 is added:

‘*Appendix 4*

Conditions and procedure to access vehicle OBD information

1. Scope

1.1. This Appendix contains the conditions for access that the manufacturer shall only be allowed to set out and procedures that the vehicle manufacturer shall apply or shall only be allowed to require other parties to apply, while implementing the security measures for access to OBD information referred to in points 2.9.(a) and (b) of this Annex.

1.2. Any reference in this Appendix to independent operators or to manufacturer’s authorised partners, dealers and repairers, as well as to a vehicle manufacturer acting for repair and maintenance purposes in this Appendix shall include any person or operator acting on their behalf, such as a service provider performing remotely, as a service provided to the independent operator, the programming, fitting or activating of parts and equipment on a vehicle (remote service suppliers).2. Obligations of the manufacturer

2.1. The vehicle manufacturer shall be responsible for ensuring that all technical prerequisites for the application of the procedures referred to in this Appendix are in place, including access credentials such as certificates or software tokens and necessary arrangements with diagnostic tool manufacturers.

2.2. The vehicle manufacturer shall demonstrate to the approval authority that the vehicle is designed to enable access to OBD information, in compliance with the requirements of this Appendix, using multi-brand diagnostic tools.

2.3. The vehicle manufacturer shall provide to the manufacturers of diagnostic tools the information referred to in point 11 of this Appendix.

2.4. The vehicle manufacturer shall ensure that its server used for the purpose of enabling access to OBD information offers to independent operators, on a non-discriminatory basis, the same availability and performance of the information system as it offers to its authorised partners, dealers and repairers or is used by the manufacturer for the purpose of enabling access to OBD information.

Vehicle manufacturer shall ensure that any server used for the purpose of enabling independent operator access to OBD information is accessible without interruption, except for exceptional and unforeseeable circumstances outside the vehicle manufacturer's control and not attributable to negligence on its part, or as required for maintenance purposes of the information system.

The vehicle manufacturer shall make yearly server availability statistics information available to the approval authority upon request.

2.5. The vehicle manufacturer shall not restrict access to OBD information beyond the restrictions laid down in this Appendix unless specifically provided otherwise in this Regulation. Furthermore, the vehicle manufacturer shall not restrict access by independent operators to OBD information beyond the restrictions applicable to its authorised partners, dealers and repairers or to the vehicle manufacturer accessing the OBD information for repair and maintenance purposes.

2.6. The Vehicle manufacturer shall ensure that the cybersecurity measures they implement, including the compatibility requirements referred to in point 6.2, do not result in restricting or obstructing access to OBD information under this Appendix beyond what is necessary and proportionate to comply with Article 4.5(d) and Annex II line D4 of Regulation (EU) 2019/2144. Such measures may address future risks and threats where the vehicle manufacturer can demonstrate their impact and probability.

2.7. Any measures implemented by vehicle manufacturer to prevent emissions tampering and the odometer fraud shall not restrict or obstruct access to the OBD information beyond what is necessary and proportionate to comply with Articles 4(7) and 4(8) of Regulation (EU) 2024/1257.

3. Authentication

3.1. The vehicle manufacturer may, as a condition for issuing the access credentials, require authentication of the diagnostic tool manufacturer and the diagnostic tool used, except for the following repair and maintenance operations :

(a) reading diagnostic trouble codes;

(b) reading the vehicle VIN;

(c) reading data and clearing diagnostic trouble codes where unrestricted access by means of a generic or OBD scan-tool is either required under Regulation (EU) No 2017/1151 or Regulation (EU) No 2024/1257; or provided for in UN Regulation No 49, UN Regulation No 83*, UN Regulation 168** or UN Regulation No 154.

3.2. Whenever access to OBD information involves changes to the vehicle, the vehicle manufacturer may , as a condition for issuing the access credentials, require

authentication of the operator. In the case of devices used for monitoring purposes, where data is only read and autonomously reported to the diagnostic tool manufacturers server without any human interaction, the vehicle manufacturer shall not require authentication of the operator .

3.3. Where access to OBD information involves a change of the vehicle software or its configuration/its parameters consisting in reprogramming of the vehicle software code, resulting in alteration of the intended behaviour of the vehicle and persisting beyond the repair and maintenance operation, so that it can only be reversed or overwritten by the performance of an equivalent operation, the vehicle manufacturer may require authentication of the employee of the operator who is seeking to access OBD information, unless the manufacturer of the diagnostic tool attests to the vehicle manufacturer that, based on the result of an independent audit performed no earlier than 3 years before the request, the operator has a system in place allowing for unambiguous identification of the employee seeking such access.

3.4. Cases of access referred to in point 3.2 shall include such repair and maintenance operations as activation of actuators and functional test routines, clearing of diagnostic trouble codes, resetting of service lights, resetting of adaptive learning parameters, and replacement of parts including initialisation of non-smart component and reading data by identifier, except where it is used for the purposes of Periodic Technical Inspection with values comparable to the values defined in ISO20730-3, Annex B, provided that these values are available in the vehicle.

3.5. Cases of access referred to in point 3.2. shall include calibration, understood as a process of adjusting or aligning vehicle software and hardware parameters as prescribed by the vehicle manufacturer and without variant coding or modifying the vehicle software.

3.6. For the purposes of authentication referred to in points 3.1 to 3.3., the manufacturer of the tool used to access the OBD information may be required by the vehicle manufacturer to attest to the vehicle manufacturer the following:

(a) the identity of the diagnostic tool,

(b) where access to OBD information involves changes to the vehicle referred to in point 3.2, the identity of the diagnostic tool and pseudonymized identity of the operator and the compliance of the operator with the authorization requirements referred to in point 8.1.,

(c) where access to OBD information involves a change of the vehicle software or its configuration/its parameters consisting in reprogramming of the vehicle software code, resulting in alteration of the intended behaviour of the vehicle and persisting beyond the repair and maintenance operation, so that it can only be reversed or overwritten by the performance of an equivalent operation, as referred to point 3.3, the pseudonymised identity of the operator’s employee and the compliance of this employee with the authorisation requirements referred to in point 8.2.

3.7. In cases referred to in point 3.6. point b) and c), the identity of the operator and, where relevant, the employee of the operator and their compliance with the authorization requirements referred to in points 8.1. and 8.2. shall be verified by the manufacturer of the diagnostic tool used to access the OBD information or established based on an authorization certificate referred to in point 9.2.

3.8. No fees shall be required by the vehicle manufacturer for access to vehicle OBD information under point 2.9. of Annex X. However, vehicle manufacturer may charge justified and proportionate fees for the use of the remote facility referred to in point 2.9 point c).

4. Connection requirements

4.1. Except for cases of access referred to point 3.1, points (a) to (c), the vehicle manufacturer may require one-time online connection from the diagnostic tool through diagnostic tool manufacturer's server to vehicle manufacturer's server to receive credentials. After the provision of access credentials, access shall not require online connection.

4.2. Whenever access to OBD information involves a change of the vehicle software or its configuration or its parameters resulting in alteration of the intended behaviour of the vehicle that persists beyond the repair and maintenance operation and that can only be reversed or overwritten by the performance of an equivalent operation, the vehicle manufacturer may require a continuous online connection at the time of performing the repair from the diagnostic tool to diagnostic tool manufacturer's server as well as from the diagnostic tool manufacturer to the vehicle manufacturer server.

4.3. Cases of access referred to in point 4.2. shall include the following;

(a) repair and maintenance operations as setting up a replacement component and customer preferences, identifying an Electronic Control Unit (ECU) and variant coding, initialising an ECU and a component, variant coding when replacing existing components, and variant coding when adding a new component;

(b) repair and maintenance operations referred to in point 5.5.

4.4. Cases of access referred to in in point 4.2 shall not include repair and maintenance operations enumerated in points 3.4 and 3.5.

4.5. However, by way of derogation from the point 4.4., cases of access referred to in point 4.2. include repair and maintenance operations referred to in point 3.5. where it is necessary to validate calibration values which are subject to regulatory requirements or where calibration cannot be completed without individual

component or separate technical unit specific data necessary to complete the repair process and retrieved from the manufacturer's server as part of a variant coding process.

5. Traceability requirements

5.1. Except for cases of access referred to in points a) to c) of point 3.1 , the vehicle manufacturer may require the diagnostic tool manufacturer to collect and store the vehicle VIN and the unique diagnostic tool identifier.

5.2. Whenever access to OBD information involves changes to the vehicle , the vehicle manufacturer may require the diagnostic tool manufacturer to collect and store all executed diagnostic jobs (e.g. service-ID and sub-function) and used parameters/attributes UTC date and time stamps for each interaction with the vehicle.

5.3. Cases of access referred to in point 5.2. shall include such repair and maintenance operations as those referred to in points 3.4., 3.5., 4.3. and 4.6.

5.4. Whenever access to OBD information involves a change of the vehicle software or its configuration/its parameters consisting in reprogramming of the vehicle software code, resulting in alteration of the intended behaviour of the vehicle and persisting beyond the repair and maintenance operation, so that it can only be reversed or overwritten by the performance of an equivalent operation, the vehicle manufacturer may require the diagnostic tool manufacturer to collect and provide the results of the vehicle network topology inspection, initial vehicle state upon connection, including hardware/software versions of all electronic control units installed in the vehicle, results of all module interaction and routines run (e.g. return parameters) and results of the post-repair final vehicle health check readout.

5.5. Cases of access referred to in point 5.4. shall include such repair and maintenance operations as pairing an original replacement part (including software and hardware compatible (as defined by the vehicle manufacturer) remanufactured or re-used part) or a vehicle manufacturer authorized replacement part to a vehicle using an independent diagnostic tool and reprogramming a module using original equipment vehicle software and original equipment programming software in accordance with the vehicle manufacturer's instructions.

5.6. Cases of access referred to in in point 5.4. shall not include repair and maintenance operations enumerated in points 3.4., 3.5., 4.3. and 4.6.

6. Cybersecurity requirements applicable to diagnostic tool

6.1. Except for cases of access referred to in points a) to c) of point 3.1, the vehicle manufacturer may require that the diagnostic tool used to access the OBD information comply with the relevant requirements of Regulation (EU) 2024/2847 and that the diagnostic tool manufacturer comply with either Trusted Information Security Assessment Exchange (TISAX), to the level specified by the vehicle manufacturer in compliance with point 2.5, or ISO 27001.

6.2. Whenever access to OBD information involves changes to the vehicle referred to in point 3.2., the vehicle manufacturer may require that the diagnostic tool used to access the OBD information and the diagnostic tool manufacturer comply with the requirements of the vehicle manufacturer's security implementation.

6.3. The requirements of the vehicle manufacturer's security implementation shall not exceed the requirements imposed on vehicle manufacturer's own diagnostic tool, tool suppliers and own organisation and shall be applied on a non-discriminatory basis.

6.4. The vehicle manufacturer may require the diagnostic tool manufacturer to perform tests to verify the compliance of the diagnostic tool with the specified requirements. A Service Level Agreement shall ensure that any verification of the results of these tests performed by the vehicle manufacturer is done in a timely manner. In case a diagnostic tool manufacturer's compliance with the requirements of this section is not confirmed, a clear statement of the reasons for non-compliance shall be provided by the vehicle manufacturer, together with the required measures to be implemented by the diagnostic tool manufacturer.

6.5. Cases of access referred to in point 6.2. shall include such repair and maintenance operations as those referred to in points 3.4., 3.5.

6.6. Whenever access to OBD information involves change of the vehicle software or its configuration/its parameters resulting in alteration of the intended behaviour of the vehicle persisting beyond the repair and maintenance operation, so that it can only be reversed or overwritten by the performance of an equivalent operation, the vehicle manufacturer may require that the diagnostic tool used to access the OBD information and the diagnostic tool manufacturer comply with the relevant requirements of the vehicle manufacturer's Software Updates Management System (as defined in UN Regulation No 156[***])implementation. Those requirements shall not exceed the requirements imposed on vehicle manufacturer's own diagnostic tool, tool suppliers and own organisation and shall be applied on a non-discriminatory basis.

6.7. Cases of access referred to in point 6.6. shall include such repair and maintenance operations as those referred to in points 4.3., 4.6. and 5.5. and shall not include those referred to in points 3.4. and 3.5.

7. Access credentials

7.1. Where all the conditions referred to in sections 3, 4 and 6 are complied with, the vehicle manufacturer shall, without delay, provide the diagnostic tool manufacturer with access credentials sufficient to enable the access to the required OBD information.

7.2. Access credentials may be VIN-specific.

7.3. Access credentials shall be valid for at least 30 days from the time of provision.

7.4. However, whenever access to OBD information involves a change to the vehicle, the vehicle manufacturer may limit the validity of access credentials to 24 hours.

7.5. Cases of access referred to in point 7.4. shall include such repair and maintenance operations as those referred to in points 3.4., 3.5., 4.3., 4.6. and 5.5.

8. Authorisation criteria and authorization certificates

8.1. In cases referred to in point 3.2., the vehicle manufacturer may refuse to issue access credentials if the manufacturer of the diagnostic tool used to access the OBD information does not attest that the operator seeking access to OBD information:

a) has a valid liability insurance with a minimum amount of coverage of EUR 1 million for bodily injury and EUR 0,5 million for property damage;

b) pursues a legitimate business activity in the automotive sector as referred to in point 6.3 of this Annex;

No other conditions for issuing access credentials shall be imposed by the vehicle manufacturer than those specified in points(a) and (b).

8.2. In cases referred to in point 5.4, where the vehicle manufacturer requires the authentication of the employee of the operator and unless the manufacturer of the diagnostic tool attests to the vehicle manufacturer, in compliance with the conditions set out in point 3.3, that the operator has a system in place allowing for unambiguous identification of the employee seeking such access, the vehicle manufacturer may refuse to issue access credentials if the manufacturer of the diagnostic tool used to access the OBD information does not attest, in addition to the conditions referred to in point 8.1., that the employee seeking access to OBD information holds an employment agreement with the operator seeking access to OBD information and

that the employee concerned has a valid country specific identity card or an equivalent document.

8.3. To be eligible for the authentication procedure under this Appendix, the diagnostic tool manufacturer shall have committed in the general conditions of contracts with operators to accept on request by the independent operator, for the purpose of attesting the compliance with the requirements referred to in points 8.1 and 8.2., a certificate referred to in point 9.2 of this Appendix and issued not earlier than 60 months before the request for access.. However, where the operator does not request to be authenticated based on such a certificate, the diagnostic tool manufacturer may, for the purpose of authentication, choose to verify the identity of the operator or the operator's employee and the compliance with the authorization criteria by its own processes.

9. Conformity Assessment Body and Trust Centre

9.1. Certificates referred to in points 3.7. and 8.3. shall be issued by a Trust Centre referred to in point 2.1.6. of Appendix 3 based on the findings of a conformity assessment body as referred to in point 4.2.2. of Appendix 3 with regard to the circumstances referred to in point 9.2.

9.2. For the purpose of issuing the authorization certificates by a Trust Centre, the Conformity Assessment Body shall:

a) comply with the requirements referred to under points (a), (b), (d), (e), (f), (g), (h), (i), (k), (l), (n), and (p) of point 4.3.1. of Appendix 3 of Annex X;

b) inspect and confirm the circumstances referred to under (d) and (g) of point 4.3.3 of Appendix 3 of Annex X. In cases referred to in point 5.4, where the vehicle manufacturer requires the authentication of the employee of the operator, the inspection and confirmation of those circumstances shall refer to the employee of the operator.

9.3. For the purpose of issuing authorisation certificates in cases referred to in point 9.1., Trust Centre shall:

a) comply with the requirements of point 4.6 of Appendix 3

b) provide all required information to the diagnostic tool manufacturer to implement the certificates into their diagnostic tools.

10. Vehicle manufacturer's access to information concerning the operator

10.1 The vehicle manufacturer shall obtain, on request, from the manufacturer of the diagnostic tool access to the information regarding an individual repair or maintenance operation recorded in accordance with section 5 only where this is necessary in relation to repair or maintenance work carried out on an individual vehicle to:

a) react to a reasonable suspicion of serious misuse of access to the vehicle,

b) carry out investigations in case of product liability or warranty claims

c) investigate cybersecurity or illegal tampering incidents, answer queries of the vehicle owner or a public authority

In cases referred to in points b) and c), this information shall include, where applicable, the information regarding the operator and/or its employees. In cases where the manufacturer of the diagnostic tool relied for the authentication on a certificate provided by the Trust Centre, the relevant CAB shall provide the required information based on its assessment of a documented request by the vehicle manufacturer.

The vehicle manufacturer shall ensure that the information regarding an individual repair or maintenance operation accessed for the purposes referred to in points a) to c) shall not be used for any other purpose.

10.2. In cases referred to in point 10.1, the manufacturer of the diagnostic tool shall inform, without delay, the independent operator and, where relevant, the employee of the independent operator, about the access to the information regarding an individual repair or maintenance operation or to the information concerning the operator and/or its employees.

10.3. In cases referred to in points a) and c) of point 10.1. and where this is necessary and proportionate to prevent further misuse or address cybersecurity risk, the vehicle manufacturer may temporarily suspend or restrict access of the diagnostic tool concerned or request the involved manufacturer of the diagnostic tool to take immediate measures to temporarily restrict the access of the concerned operator, diagnostic tool, or employee to the OBD information concerning the vehicles of this manufacturer.

10.4. In exceptional cases, in response to a significant present or imminent cybersecurity incident a Vehicle Manufacturer may suspend access to the OBD information, at the most granular level possible, where it is necessary and proportionate to respond to the incident concerned.

10.5. In cases referred to in points 10.3 and 10.4, the vehicle manufacturer shall, at the same time, notify the suspension to the Approval Authority, together with the reasons for the suspension and all relevant evidence. The suspension shall be lifted when the incident is settled or if the Approval Authority requests the vehicle manufacturer to do so.

The Approval Authority shall, within 10 days from the day of the notification, review the grounds for suspension and, if the suspension is manifestly unjustified or disproportionate, request the vehicle manufacturer or the involved manufacturer of the diagnostic tool] to restore access

The Approval Authority may, at any time, request the vehicle manufacturer and the involved manufacturer of the diagnostic tool to restore access where it considers that the grounds for suspension ceased to exist.

11. Information to be provided to diagnostic tool manufacturers

11.1. The vehicle manufacturer's RMI system shall display contact data and process information on how to obtain the requested information, as specified in points a), b), c) and d), concerning integration of diagnostic tool, at the time of the type-approval.

a) Contact information for technical and commercial enquiries

b) Description of the integration process including indicative timeline

c) General terms and conditions for integration of diagnostic tools by the diagnostic tool manufacturer

d) Schedule of fees for integration related services

11.2. Subject to the conclusion of a non-disclosure agreement, the vehicle manufacturer shall make available, on request, the following information to any independent operator complying with TISAX, to the level specified by the vehicle manufacturer in compliance with point 2.5, or ISO 27001:

a) for reference, a model agreement on security integration, clearly indicating the terms intended to be included in all the vehicle manufacturer's agreements with diagnostic tool manufacturers on this matter,

b) description of the requirements and processes for secure integration of the diagnostic tool including the indicative timeline.

11.3. The vehicle manufacturer shall provide the following information and make available the following services to the manufacturer of diagnostic tool, at the time of the conclusion of an agreement on the integration of diagnostic tool:

a) detailed and timely updated requirements, processes and technical specifications for secure integration of the diagnostic tool, including the security implementation requirements;

b) against reasonable remuneration, as referred to in point 2.3., instant response technical support for security integration and diagnostic tool verification.

11.4. The security implementation requirements referred to in point 11.3. shall be accompanied by the explanation of the reasons for this requirement. In exceptional cases the vehicle manufacturer may provide only the necessary requirements without detailed explanations where:

a) disclosing the specific objectives behind a requirement could compromise proprietary information or trade-secrets, or

b) the disclosure of the reasoning would reveal a broader cybersecurity strategy that must remain confidential to maintain the integrity of the system.

11.5. The information referred to in points 11.1 to 11.3 shall be provided together with the application for a type approval.

12. OBD Forum

12.1. The Forum on Access to Vehicle Information (OBD-Forum) shall be in charge for coordinating and monitoring the implementation of the procedures for:

a) authentication and authorisation of independent operators as described in point 3 and 8 of this Appendix, including the processes used by the manufacturers of diagnostic tools for verification of authorisation criteria, as described in point 3 of this Appendix

b) issuing access credentials as described in point 7 of this Appendix including the fulfilment of traceability and connectivity requirements,

c) disclosing the information on access and suspension or restriction of access as described in point 10 of this Appendix.

12.2. The Forum shall:

a) advise the Commission on implementation of this Appendix;

b) advise the approval authorities on disputes concerning the interpretation and implementation of this Appendix.

c) advise the vehicle manufacturers, diagnostic tools manufacturers and independent operators on:

(i) interpretation of the Appendix;

(ii) practical aspects of the procedures referred to in points 12.1;

(iii) guidance on resolving disputes concerning the implementation of the procedures referred to in point 12.1.

12.3. The members of the OBD-Forum shall be represented by vehicle manufacturers and independent operators engaged in the implementation and use of procedures and processes described in paragraph 12.1.

12.4. The OBD Forum shall operate under the common legal and organizational structure as the ‘Forum for Access to Security-Related Vehicle RMI. referred to in paragraph 2.1.12 of Appendix 3’

∗Regulation No 83 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of vehicles with regard to the emission of pollutants according to engine fuel requirements (OJ L 42, 15.2.2012, pp. 1–207, ELI: https://eur-lex.europa.eu/eli/reg/2012/83/oj/)

** Regulation No 168 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of light duty passenger and commercial vehicles with regards to real driving emissions (RDE) [2024/211] (OJ L, 2024/211, 12.1.2024, ELI: http://data.europa.eu/eli/reg/2024/211/oj)

*** Regulation No 156 of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system [2021/388] (OJ L 82, 9.3.2021, pp. 60, ELI: https://eur-lex.europa.eu/eli/reg/2021/388/oj)