Submitted by ALLIANZ, DEKRA, EVU, FSD, TH INGOLSTADT, VdTÜV

EDR and DSSAD: Table of criteria

		EDR for conventional vehicles	EDR for ADs	DSSAD for ALKS
System				
	Purpose (why do the contracting parties want to introduce this function into the vehicle?)	• Accident analysis • [conducting road safety analysis] • [assessing effectiveness of specific measures taken] • To clarify legal responsibility in complex accident scenarios		Clarify if the system or the driver • Was, or • Was requested to be in dynamic control of the vehicle at a certain time, **for the sake of legal responsibility**
	What it shall/<u>should not do</u>	• Detect who is driving • [Identifying the owner/holder of the vehicle on the basis of the stored data.]	[Identifying the owner/holder of the vehicle on the basis of the stored data.]	Provide data on accident
	PTI	• Manual triggering for storing a data set (see system „event definition“) • Retrieval of data shall be able for legally mandated road worthiness testing, in order to proof functionality of EDR		• For legally mandated roadworthiness testing access shall be at least to the most recent DSSAD data set to test the functionality of the DSSAD.

			• (The access can be protected by authorization certificates if necessary.)
	System storage capabilities	• Minimum storage volume should include 3 events in the vehicle • Storage of further events on independent backend possible (depending on national legislation of the Contracting Parties) • Ensure complete transmission to independent / sovereign backend server • Storage duration and deletion capability adaptable to CP according to national legislation	• Minimum storage volume according to ALKS (ACSF) in the vehicle • Ensure complete transmission to independent / sovereign backend server • Storage duration and deletion capability adaptable to CP according to national legislation
	System crash survivability	Resistance to R94 crash test	
	“event” definition	• “Event” means a crash or other physical occurrence that causes the trigger threshold to be met or exceeded, or an airbag to be deployed, whichever occurs first. • Manual triggering of storing of a data set must be possible (Automatically stored data set shall not be over written) • Any stop of the vehicle (automatic deletion, if the vehicle was moved over a distance exceeding 300 meters and no manual storage was triggered)	Event means switches of the HAD system from a status to another status, Transition Demand by the HAD system and their nature (visual, audible, haptic), a Minimum Risk Maneuver by the HAD system and it´s end,

				a Take-Over by the human driver and receiving C-ITS signals during the HAD system is activated.
	Battery restitution	All data mandatory in the table must be stored after an event.		ACSF to confirm what they expect.
	Environmental robustness (vibrations, etc.)	• Resistance to R94 crash test	• Resistance to R94 crash test; • Fire resistance F30 + (DIN EN 13501 – 1) • Waterproof IP6k6k	
	Malfunction detection	• Tell-tale / Warning message --> for driver • Retrievable via electronic vehicle interface --> for repair purposes and roadworthiness testing		Input from ACSF is expected
Data technique				
	Where to store (in the vehicle vs. the cloud)	• The data set shall be stored in the vehicle. • If the vehicle is equipped with an over the air (OTA) communication interface, the data set shall be transmitted to an independent backend (cloud) when an active and secure network communication is available.	• The data set shall be stored in the vehicle. • The vehicle shall be equipped with an over the air (OTA) interface. • If an active and secure network communication is available, the data set shall be transmitted to an independent backend (cloud). • After successful transmission, the data set	• The data set shall be stored in the vehicle. • The vehicle shall be equipped with an over the air (OTA) interface. • If an active and secure network communication is available, the data set shall be transmitted to an independent backend (cloud).

		• After successful transmission, the data set shall be deleted from the vehicle's internal memory.	shall be deleted from the vehicle's internal memory.	• After successful transmission, the data set shall be deleted from the vehicle's internal memory.
	Data format	Standardised		
	Data element	• From 2022 until 2025 see table: EDR-DSSAD-01-02 (EVU_20190904) Table of EDR parameters until 2025 Changes to current US version marked in red color • From 2025: like AD	• Until 2025 only for HAD vehicle, after 2025 for all vehicles see Table: EDR-DSSAD-01-02 (EVU-FSD) Table of EDR Parameters for AD_20190904_1200	Time and position information for the following data elements: 1) Switches of the HAD system from a status to another status ("Activated", "Manual / automatic deactivated") 2) Transition Demand by the HAD system and their nature (visual, audible, haptic) 3) Reason of Transition Demand (e.g. technical failure of which system, planned / unplanned event) 4) Driver availability 5) Minimum Risk Maneuver by the HAD system and end

				of this Minimum Risk Maneuver 6) Take-Over by the human driver 7) Receiving C-ITS signals
	Storing duration	• Standardized as in CFR 49 Part 563 • No deletion of data set, unless vehicle has moved 300 m after last stop of the vehicle, thus driver can save data manually as long the car	• Standardized as in CFR 49 Part 563 • Depending on national or regional legislation of Contracting Parties • Preferably data deletion in vehicle EDR after successful data transmission to independent / sovereign backend	• Depending on national or regional storage periods of Contracting Parties • Premature data deletion in the in-vehicle DSSAD memory after successful data transmission to independent / sovereign backend.
	Retrieval means	• Standardised access via an electronic vehicle interface • See “access means” (if over the air (OTA) communication interface is provided)	• Standardised access via an electronic vehicle interface • Standardized transmission from the vehicle to an independent backend • See “access means”	• Standardised access via an electronic vehicle interface • Standardized transmission from the vehicle to an independent backend • See “access means”
	Accuracy	• From 2022 until 2025 see table: EDR-DSSAD-01-02 (EVU_20190904) Table of EDR parameters until 2025	• See Table: EDR-DSSAD-01-02 (EVU-FSD) Table of EDR Parameters for AD_20190904_1200	• As the AECS accuracy: Paragraphs 7.3.5., 7.3.7. to 7.3.10. of position determination shall

		Changes to current US version marked in red color • From 2025: like AD		therefore be taken from Regulation R144. • Accuracy shall be provided for the complete speed range of the automated driving function
	Access means	• In vehicle for Type Approval Authorities, Technical Services, PTI and authorized parties by means of authorization certificate. • For authorized parties additionally via independent / sovereign backend after authorization.		
	Erasing means (?)	• Complete deletion at the end of the respective storage period in accordance with national legislation on the backend, so that access / recovery is no longer possible for any party. • The data set in the EDR itself must be deleted after successful transfer to the backend. Here too, no party may be able to access, read or recover the data set.		• Complete deletion at the end of the respective storage period in accordance with national legislation on the backend, so that access / recovery is no longer possible for any party. • The data set in the DSSAD itself must be deleted after successful transfer to the backend. Here too, no party may be able to access, read or recover the data set.

	Sampling rate	• From 2022 until 2025 see table: EDR-DSSAD-01-02 (EVU_20190904) Table of EDR parameters until 2025 Changes to current US version marked in red color • From 2025: like AD	• See Table: EDR-DSSAD-01-02 (EVU-FSD) Table of EDR Parameters for AD_20190904_1200	• Like AECS R144 (<1/s)
	Data identification (this data really belongs to that vehicle)	• When retrieving the data out of the vehicle, the respective data set can generally be assigned to the VIN. • When transferring the data stored on the independent backend, the data identification depends on the respective authorization. • For accident research purposes, for example, the data may only be transmitted anonymously. This can be guaranteed by deleting the last 4 digits of the VIN.		

	Triggering parameter	• Change in vehicle velocity in either longitudinal or lateral direction that equals or exceeds 8 km/h within a 150 ms interval (i.e.: CFR 49 Part 563) • "Pedestrian" Detection Sensor • Rollover Sensor • Change in acceleration, which is able to determine an impact to the vehicle • Manually by driver • Any stop of the vehicle shall trigger the storage of a data-set according CFR 49 Part 563, but this data set will automatically be deleted, if the vehicle moves a distance exceeding 300 m, unless driver triggers manually	• Change in vehicle velocity in either longitudinal or lateral direction that equals or exceeds 8 km/h within a 150 ms interval (i.e.: CFR 49 Part 563) • Any sensor or sensor fusion data, which is able to detect an impact to the vehicle (*„Sensor fusion data means the processing of all available sensor data within the car or external, which allows the system of the car to derive additional information on a specific traffic situation (e.g. an accident)"*) • Change in acceleration, which is able to determine an impact to the vehicle • Manually by driver • Any stop of the vehicle shall trigger the storage of a data-set according CFR 49 Part 563, but this data-set will automatically be deleted, if the vehicle moves a distance exceeding 300 m, unless driver triggers manually	• See "event definition" and "data element". • Triggering parameters are the respective data elements for which a storage with time stamp and position information must be initiated.

Data usage				
	Data ownership	Vehicle owner / driver		
	Data protection (privacy)	• Retrieval and reading of the data set is only permitted for authorized parties, including vehicle owner / driver • Anonymized storage on backend • Data protection-compliant deletion, • Independent authorization and access management in compliance with the highest IT security standards • Further processing of anonymised data for research purposes		
	Information to the user (driver, vehicle owner)	1) A statement that the vehicle is equipped with a EDR and information about the purpose of the EDR. 2) The possibility that and how the EDR can be manually triggered in a distance-oriented memory range 3) Information that manual deactivation of the EDR is not possible and that permanent tracking of the vehicle does not take place. 4) Information about the data set elements, described in paragraph 5.1., the data capture, storage and survivability as	1) A statement that the vehicle is equipped with a EDR and information about the purpose of the EDR. 2) The possibility that and how the EDR can be manually triggered in a distance-oriented memory range 3) Information that manual deactivation of the EDR is not possible and that permanent tracking of the vehicle does not take place. 4) Information about the (extended) data set elements (*EDR for CV, video data, etc*), the data capture, storage and survivability as well as the data retrieval. 5) Additional information about data storage and rules on privacy and data protection,	1) A statement that the vehicle is equipped with a DSSAD and information about the purpose of the DSSAD. 2) Information about no manual deactivation and no permanent tracking of the vehicle 3) Information about the data set elements, the data storage and the data retrieval. 4) Additional information about data storage and rules on privacy and data protection, according to national

		well as the data retrieval. 5) Additional information about data storage and rules on privacy and data protection, according to national or regional legislation.	according to national or regional legislation.	or regional legislation.
	Who must access which data?	1) Type Approval Authorities and Technical Services: Data set for compliance type approval purposes; 2) Roadworthiness / PTI: Data set required for the purpose of verifying the correct functioning (storage taking place) and integrity of the EDR and the plausibility of the stored data set. 3) Authorized parties to specific datasets In addition, the precise design of the question of who gets access to which data is not content for UN ECE regulation, scope of the access regulation under national legislation.		1) Type Approval Authorities and Technical Services: Data for compliance type approval purposes; 2) Roadworthiness / PTI: Data required for the purpose of verifying the correct functioning (storage taking place) and integrity of the DSSAD and the plausibility of the stored data set. 3) Authorized parties to specific datasets In addition, the precise design of the question of who gets access to which data is not content for UN ECE regulation, scope of the access regulation

			under national legislation.
	Plausibility	• Within the scope of type approval • Via classical accident analysis • During vehicle life cycle roadworthiness testing	• Within the scope of type approval • During vehicle life cycle, the plausibility of the time stamp and position as well as the accuracy of the data set within the scope of roadworthiness testing
	Authorization process	If the data set is stored in the vehicle: • Access to the vehicle may be protected by certificates • The certificates have to be provided by the OEM to Type Approval Authorities, Technical Services, Roadworthiness authorities and authorized parties. If a data set is stored in the cloud: • Authentication and authorization via authority or authority with a sovereign task; proof of authorization via web service; • Encrypted data transmission • Concrete structure and scope of the authorization process through national legislation	
	How fast to deliver the data to a third party	• Immediately after authorization has been proven via authorization certificate	
	Cybersecurity	• End-to-end protection between the vehicle and independent backend	