

ELU_2025_003 Asset connectivity API solution - Service Level Agreement

This Services Framework Agreement (the “**Agreement**”) is made with effect as of 15th of November 2025,

BETWEEN

- I. **Enovos Luxembourg S.A.**, a *société anonyme* incorporated and existing under the laws of Luxembourg, having its registered office 2 rue Thomas Edison, L-1445 Strassen, registered with the Luxembourg Trade and Companies’ Register under registration number B 44.683, hereby represented by Mr Claude Simon, Head of Sales BU and Mr Mustafa Öztürk, Chief Information Officer,

Hereinafter referred to as the “**Client**”,

ON THE ONE HAND

AND

- II. **xx**, under company registration number **xx**, with registered address at **xx** hereby represented by **xx**,

Hereinafter referred to as the “**Service provider**”

ON THE OTHER HAND

The Service provider and the Client are hereinafter collectively called “**Parties**” and individually called “**Party**”.

Preamble

The Client is Enovos Luxembourg, main energy supplier in Luxembourg for private and professional customers. The Service provider is **[Name of the Supplier]**, a software company developing and operating a platform (“Supplier Platform”) that allows applications to communicate with internet-connected hardware such as electric vehicles. The Supplier offers API access (the “API”) to the Supplier Platform, which enables third parties to use the capabilities of the Supplier Platform. The Supplier Platform is defined as the functionality described under **‘Supported devices’ in [Link to documentation]**.

The Parties intend to enrich our enovos app and customer portal with data related to energy devices. The first use case includes electric vehicles.

IT IS THEREFORE AGREED AS FOLLOWS:

Article 1- Elements of the Agreement and their priority

The Service Level Agreement (hereinafter the “Agreement”) is composed of the present general clauses as well as of the Annexes which are part of the Agreements with the following order of priority

1. The Invitation to tender ELU_2025_003 - Asset connectivity API solution – CDC and ELU_2025_003 Asset connectivity API solution - Technical Annex
2. This Service Level Agreement
3. The data processing appendix in Annex 1
4. The offer from the Service Provider in Annex 2

Article 2 – Scope of the Services

The Client instructs the Service Provider with the providing of services, in particular the following services (“Services”) in Enovos mobile app and in Enovos customer portal:

- Onboarding: plan and kick-off the initial use cases
- Development: start and support integration with Service Provider API
- Testing: build, test and iterate with users
- Launch and scale: support the launch of products
- Monitoring and support: provide continuous monitoring and support throughout all phases to ensure smooth execution and address any challenges effectively.
- Advisory: provide expert guidance and strategic recommendations to optimize API usage, enhance performance, and ensure alignment with business objectives. Offer insights on best practices, industry trends, and potential improvements to maximize the value derived from the API integration.

The content, the scope, the modalities, the price and/or as the case may be, the remuneration modalities of such provided services are fixed in the Annexes. The Parties may at any time agree on the providing of other services which are not included in the above list by agreeing on further annexes which will be part of the Agreement. All Annexes and all agreements posterior to the date of the present agreement shall be made in written form and signed by the Parties. No verbal agreement will bind the parties.

Article 3 – Price of the services

3.1 The prices of the Services are based on monthly fixed fee and usage licenses per [active user or active device] per month. The model for usage licenses will depend on the offer selected by the Client.

3.2 The prices of the Services are mentioned in Annex 2.3.3.. In case of contract extension as defined in the article 6, the initial prices of the Services are kept. No price adaptations will be permitted.

Article 4- Invoicing and payment

4.1 The Services will be invoiced on a monthly basis.

4.2 The invoices are payable within thirty days (30) after the end of the month in which the invoice is received.

4.3 In case of non-payment, late payment interest rates are due thirty days after receipt of the invoice, in accordance with the law dated 18 April 2004 regarding payment deadlines and late payment interests, as amended.

4.4 The invoice must be sent electronically to the following e-mail address:

TO: AP-enovosluxembourg@encevo.eu

CC : antonio.carvalho@enovos.eu / emma.korchia@enovos.eu / ivan.Deschamps@enovos.eu

Article 5 - Bank Account

The payments are effected on the following EUR bank account of the Service Provider,

Name of the Bank:

Address:

Account Holder:

Account Number:

IBAN:

SWIFT code:

Article 6 - Duration of the Agreement

6.1. The Agreement comes into effect as of 15th of November 2025.

6.2 The Agreement and the initial Annexes are concluded for a period of 2 years starting at the start date.

6.3 If not terminated in accordance with article 7, the Agreement is tacitly extended for a 1-year period. The Agreement and the initial Annexes may be reconducted a maximum of 2 times, each for a 1-year period, unless terminated as per the provisions outlined in article 7.

6.4 In case of conclusion by the Parties of supplemental Annexes after the entry into force of the Agreement or during the periods of tacit prolongation, such Annexes will have the same duration as the Agreement itself and as a result the Agreement will always be subject to the same expiration date.

Article 7 - Termination

7.1 Without prejudice to the cases of anticipated termination, each party may terminate the Agreement including the Annexes with a delay of one (1) month preceding the beginning of a possible renewal by sending to the other party a registered mail with acknowledgment of receipt.

The termination of the Agreement triggers the termination of the Annexes.

7.2 However it is possible for the Parties to terminate, in accordance with the terms and conditions described in the first paragraph one or more Annexes. In such case, the termination of one or several Annexes will not trigger the termination of the Agreement or of the other Annexes.

7.3 Failure to meet the Technical Service Level Agreement described in Annex 2 shall entitle the Client to terminate extraordinary without any delay.

Article 8 - Anticipated termination

8.1 The Client may terminate the Agreement or one or several Annexes in the following cases:

- a) In case the solution is not technically acceptable for the expected outcome
- b) if the Service Provider is subject to liquidation, bankruptcy or similar procedures existing pursuant to existing national legislations;
- c) if the Service Provider does not respect its obligations regarding conflicts of interest;
- d) if the Service Provider made false declarations by giving the information requested by the Client;
- e) if the Service Provider cannot, due to its own fault, obtain a permit or an authorization which is necessary for the execution of the Agreement.
- f) if more than 10% of connected assets are unreachable for a period of more than 48 hours

8.2 Furthermore, each party may terminate the Agreement if one of the parties persists in not fulfilling its contractual obligations, even after having received a written formal notice indicating the nature of the supposed breach and giving a reasonable time to remedy to such breach. The time period shall be 30 calendar days in case of the non-performance of an essential obligation of the agreement.

8.3 In case a *force majeure* event lasts longer than 45 days, each Party may terminate the Agreement if its performance may not be assured after the aforementioned time period.

8.4. The termination enters into full force from the date of receipt of the registered mail with acknowledgment of receipt terminating the Agreement or from any posterior date mentioned in the termination letter.

8.5 After termination, the Client may hire any other service provider to fulfil the services.

Article 11 – Protection of personal data and data compliance :

11.1 The Parties shall comply with European regulations and national laws governing the treatment of personal data (hereafter defined the “Law”), in particular the European 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 (hereinafter referred to as the "GDPR").

11.2 Where the purpose of the Agreement is or incorporates processing of personal data as defined under the Annex I : “DATA PROCESSING APPENDIX” shall apply and be executed between the Parties:

☒ applicable,

☐ not applicable.

The Parties shall apply the obligations further detailed in Annex I. Capitalized terms used in this Article are those defined in Annex I.

11.3 As defined by the GDPR, the Client is Data Controller and the Service Provider will act as Data Processor in the treatment of the Personal Data of the Data Subjects. The Service Provider shall process the Personal Data only for the purposes defined by the Parties and in compliance with the Law, notably in accordance with the provisions of articles 28 and 32 of the GDPR and with obligations described in Annex III.

11.4 In accordance with the applicable Law, the Data Subjects can exercise their rights relating to the processing of their Personal Data by contacting the Data Protection Officer, whose contact details are provided in Annex I.

11.5 In the event of failure, breach or non-compliance of the obligations prescribed by the GDPR or of the provisions provided by the Annex I and notwithstanding anything to the contrary in the Agreement, the Service Provider shall remain liable of any damage, including any damage caused by any of its employee, any person under its direction, authority, control, liability or acting on its behalf.

11.6 The Service Provider undertakes that the application, the platform and all related services provided to the Client comply with all applicable laws and regulations, notably the Artificial Intelligence Act (EU) 2024/1689 of 13 June 2024 on artificial intelligence and the Data Act (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data, as amended from time to time.

More particularly, the Service Provider undertakes to comply with the following requirements:

- Ensure transparency about any AI system, functionalities and the disclosure of AI usage ;
- Restrict access control and implement robust data governance;
- No automated decision-making processes;
- Enable data portability and facilitate interoperability;
- Maintain human oversight and risk management monitoring ;
- Ensure availability of the documentation and record keeping.

Article 12 – Property of the results – intellectual and industrial properties.

12.1 Except for contradictory stipulations in the Annexes, all results or rights attached to the Annexes,

including all author rights (including moral rights) and other intellectual or industrial property rights, obtained within the scope of the execution of the Agreement are the exclusive property of the Client, who may exploit, publish, transfer such rights, without geographical or other limitation, subject to rights existing prior to the conclusion of the present Agreement.

12.2 Supplier shall not be limited in any way from this Agreement in further developing any parts or functionalities of the Supplier API and the Supplier Platform, or any other part of Supplier's operations. Supplier may thus, inter alia, use any insights, ideas or suggestions provided voluntarily by the Purchaser regarding the Supplier API and the Supplier Platform for new or improved developments thereof except where those are protected by article 14 of the Agreement.

Article 13 – Conflict of Interest

The Service Provider takes all necessary measures in order to preserve the Parties from any situation which could jeopardize the impartial and objective execution of the Agreement. Each conflict of interest arising during the execution of the Agreement needs to be reported immediately in written form to the Client. In case of conflict of interest, the Service Provider will immediately take all measures necessary in order to end such conflict.

Article 14 – Confidentiality

All information of whatsoever nature and of whatsoever form (for example any written document or photocopied document, any drawing, listing, disc, all figures and graphics, all recordings or any other information on whatsoever format) exchanged in the context of the Agreement are presumed to be confidential. In any case, any information regarding the financial, the information regarding strategy and the whole set of information regarding the clients of each of the Parties is confidential.

The following information is not falling within the scope of the present article:

- information which is now part of the “*domaine public*” without violation of the Agreement and its annexes, before it has been made public by one of the Parties;
- information which is published with prior written consent of the other Party;
- which publication has been ordered by judicial or administrative injunction;
- which is already known by the Parties receiving the information at the moment when the information is published, or which becomes known by such same party by another source than the other Party which has given the information, such fact will need to be proved by the party which has obtained the information from another source.

14.2 The Service Provider undertakes to treat strictly confidential all information and not to use such information neither to forward it to third parties nor to use it for its personal profit or the profit of third parties, even after the fulfilment of said tasks.

14.3 The Service Provider ensures that all its employees, administrative bodies and sub-contractors according to article 15, respect the confidential character of the information (including all **commercially sensitive information** in accordance with the “loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité” and the “loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel”) and does not divulgate such information to third parties or to use it for its personal profit or the profit of third parties, even after the fulfilment of said tasks.

Article 15 - Subcontracting

15.1 Without prejudice to article 14 and particularly its paragraph 3, the Service Provider may conclude subcontracts with third parties provided that the Service Provider enters into a confidentiality agreement with the third party in order to protect the Client's confidential information as described in article 14.

15.2 Even if the Service Provider concludes subcontracts with third parties, it is not released from its obligations towards the Client pursuant to the Agreement and he takes the responsibility of its execution.

15.3 The Service Provider will take care that the subcontract does not affect the rights and warranties of the Client pursuant to the Agreement.

Article 16 - Transfer

16.1 Service Provider may not transfer all or part of its rights and obligations resulting from the Contract without prior written consent of the Client.

16.2 In the absence of any authorization mentioned in paragraph 1 or in case of non-respecting of the conditions of such authorization, the effected transfer by one of the Parties has no effect *vis à vis* the other Party.

Article 17 – Severability Clause

In case one of the stipulations of the Agreement becomes or is declared illegal, non-applicable or null and void, the other stipulations remain effective. The Parties will use their best efforts to substitute such stipulation by another stipulation being as close as possible to the non-applicable stipulation and having an equivalent result.

Article 18 – Applicable Law – Dispute settlement

18.1 The Agreement is subject to the laws of the Grand-Duchy of Luxembourg exclusively.

18.2 In case of any dispute arising in connection with the interpretation or the application of the Agreement, the Parties will use their best efforts to find an amicable solution.

18.3 Any dispute which cannot be solved amicably shall be exclusively decided by the competent court of Luxembourg City.

Luxembourg, executed in two copies.

Place, Date:

Mustafa Öztürk
CIO of Enovos Luxembourg

[Name]
[supplier information]

Claude Simon
Head of Sales - Enovos Luxembourg

Annexe I of the contract: **DATA PROCESSING APPENDIX (“DPA”)** to the Service Level Agreement (the “Agreement”)

Article 1 Definitions

The terms used with capital letters in the data processing appendix (hereafter designated the “Appendix” or “DPA”) shall have the following meaning:

- **Agreement** shall mean the agreement referenced above, including its schedules, annexes or appendices and this DPA, forming part of the Agreement.
- **Data Controller** shall mean ENOVOS LUXEMBOURG S.A, a company incorporated and existing under the laws of the Grand-Duchy of Luxembourg, having its registered office at 2, Domaine du Schlassgoard, L-4327 Esch/Alzette, Grand Duchy of Luxembourg, registered with the Luxembourg trade and companies register under number B 44683, which determines the purpose and means of the Personal Data processing, being referred as “Client” in the Agreement.
- **Data Processor** shall mean , having its registered office at , registered with the Registry of Commerce and Companies under number , which processes the Personal Data on behalf of the Data Controller, being referred as “Supplier” or “Service Provider” in the Agreement.
- **Data Subject** shall mean the natural person whose Personal Data are being processed by the Data Processor.
- **DPO** shall mean the Data Protection Officer appointed by the Data Controller and/or by the Data Processor.
- **GDPR** shall mean the 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, and repealing Directive 95/46/EC.
- **Parties** shall mean both the Data Controller and the Data Processor.
- **Personal Data** shall mean the personal data as defined under article 4.1 of the GDPR transmitted by the Data Controller to the Data Processor within the framework of the Agreement.
- **Sub-Processor** shall mean any sub-processor subsequently engaged by the Data Processor for carrying out specific processing activities on behalf of the Data Controller under the conditions of clause 5 herein.

Unless otherwise defined herein, the definitions of the GDPR, in particular the terms “Member State”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall apply to the DPA.

Article 2 General compliance

This DPA specifies the rights and obligations of the Parties in connection with the Processing of the Personal Data.

The Data Processor acknowledges and undertakes to comply with the laws and regulations governing the processing of Personal Data, including, but not limited to, the GDPR and any other national applicable laws or regulations governing the processing any Personal Data, within the framework of the Agreement.

Article 3 Data Protection Officers

The DPOs appointed by the Parties shall be contacted by using the following information:

DPO appointed by the Data Controller:

Name: Björn Bitschnau

Address: 2, domaine du Schlassgoard,

L-4437 Esch-sur-Alzette

DPO appointed by the Data Processor:

Name: xx

Address: xx

Telephone: xx

Telephone: (+352) 2737 - 6226

Email: xx

Email: dpo@enovos.eu

Article 4 Description of the outsourced data processing operations

The Data Processor is authorized to process on behalf of the Data Controller the Personal Data necessary to provide and administrate the services and/or products, as defined in the Agreement, as follows:

- i. Categories of Personal Data concerned are contractual and personal data of customers (Identification Data (e.g., customer ID – indirectly via API authorization, Point of Delivery (“PoD”)), Contact Data (e.g., email address used during vehicle account linking), Location Data (e.g., GPS data, metering point address – if user consents), usage analytics (e.g., charging history, usage patterns), Preferences Data (e.g., smart charging configurations), Technical Data (e.g., device metadata, vehicle model, battery data). Data shared is limited to what is strictly necessary and is based on explicit consent from the user.
- ii. Subject matter and nature of the operations carried out: for the purposes of data collection, storage, analysis, and secure transfer necessary for the configuration, monitoring, and optimization of energy-related services and products, including the provision of tailored energy management solutions.
- iii. Categories of Data Subjects are retail clients
- iv. Duration of the Processing is bind to the Agreement
- v. Purpose(s) of the Processing operation(s): the purposes of processing personal data are the following :
 - a. To connect assets as electric vehicles to the application of the Data Controller;
 - b. To follow monitoring of the consumption or production data as charging data for electric vehicles and the statement per [month/year];
 - c. To obtain electronic vehicles home charging statistics;
 - d. To follow the history of charging sessions;
 - e. To enable customers who subscribed to specific energy tariff to optimize their energy costs by connecting to assets as electric vehicle, wallbox, heatpump, inverter;
 - f. To send notifications relating to asset usage as electric vehicles charging.

Article 5 Obligations of the Data Processor

The Data Processor undertakes to comply with obligations provided by article 28 of the GDPR in relation to the Personal Data, including notably the following commitments:

- i. Not to transfer the Personal Data outside of the of the European Union, nor to any international organization except (i) with the prior written acceptance of the Client and (ii) on condition that the Data Processor has provided appropriate safeguards to ensure an adequate level of data protection in accordance with articles 44 to 49 of the GDPR.
- ii. To store the Personal Data in an European Member State, to the exception of transfers outside European Union expressly authorised by article 13 of this DPA;
- iii. To process the Personal Data only for the purpose(s) for which they have been transmitted, to the exclusion of any other use;
- iv. To process the Personal Data only in accordance with the Data Controller’ documented requirements as described in the Agreement (notably not to sell, assign, lease or transfer the Personal Data to third parties). If the Data Processor considers that a request from the Data Controller or any third party constitutes a breach of the GDPR or any other applicable laws and regulations for personal data

protection, it shall immediately inform the Data Controller. In addition, if the Data Processor is required to transfer data to a third country or to an international organisation by virtue of a legal or regulatory obligation to which it is submitted, it shall inform the Data Controller of such obligation before the transfer unless the laws establishing such obligation prohibits such information for reasons of public interest.

- v. To ensure the confidentiality of the Personal Data processed within the framework of the Agreement and to take all necessary precautions, with regard to the nature of the Personal Data and the risks of the Processing;
- vi. To ensure that its employees, agents and Sub-processors who have access and/or are authorised or involved in the Processing of Personal Data have committed themselves to keep the Personal Data confidential in similar terms and conditions, are properly qualified and trained in relation to data protection;
- vii. To conduct the Processing in a professional manner and in compliance with the principles of proper data processing, notably to apply within its internal organization the principles of data protection by design and by default on its tools, products, applications and/or services;
- viii. To provide the Data Controller within reasonable delay any information necessary for the fulfilment of any required formalities and submit proof of its compliance with applicable regulations regarding the protection of Personal Data, at any moment upon the Data Controller's request;
- ix. Not to engage a Sub-Processor for carrying out specific processing activities without the Data Controller's prior consent given in writing. The information provided to the Data Controller shall include a clear description of the processing activities being outsourced, the identity and contact details of the Sub-Processor. The Sub-Processor shall comply with the provisions of the DPA and provide equivalent protections to ensure security and confidentiality of the Personal Data. The Data Processor shall remain fully liable to the Data Controller for the performance of that Sub-Processor's obligations in compliance with the GDPR and;
- x. In the event that the Data Processor is in a position to determine the purposes and means of certain Processing operations carried out on the Personal Data provided by the Client, it shall be considered as a data controller for these operations only and shall satisfy all related obligations as described in the GDPR. The Data Controller shall not be held responsible or jointly responsible for any breach of the Data Processor's obligations, when the latter is acting as data controller.

Article 6 Required technical and organizational measures

Taking into account the state of technological development, the costs of implementing such measures and the nature, scope and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons referred to in article 32 of the GDPR, the Data Processor shall implement the necessary technical and organisational measures to ensure a level of security appropriate to the risks, including inter alia as appropriate :

- (i) the pseudonymisation and encryption of Personal Data;
- (ii) the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- (iii) the ability to restore the availability and access to Personal Data in a prompt manner in the event of a physical or technical incident and;
- (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

In particular, the Data Processor shall assess the appropriate level of security by taking into account the risks that are presented by processing to prevent unauthorised or unlawful processing of the Personal Data, destruction, loss, alteration, unauthorised disclosure of, access or damage to, the Personal Data transmitted, stored or otherwise processed.

The Data Processor undertakes to require from respective Sub-Processors to establish and maintain, appropriate physical, technical and organisational measures to protect the Personal Data against the above-mentioned risks.

Article 7 Data Subject' Rights

The Data Controller will provide to the Data Subject the necessary information relating to the Processing of his/her Personal Data at the time of the Personal Data collection as required under applicable law.

The Data Controller shall be responsible for dealing with Data Subject's requests. The Data Subject shall refer to the Data Controller to assert their rights granted by the GDPR for the treatments related to the DPA ("**Data Subject Requests**").

The Data Processor shall inform promptly by email to the Data Controller's DPO and within a maximum of forty-eight (48) hours of any Data Subject's Request, without responding to such requests unless expressly otherwise instructed by the Data Controller.

To the extent possible, the Data Processor undertakes to assist in a proactive manner the Data Controller in fulfilling its obligation to respond to Data Subject's Requests, namely the right of access, rectification, erasure and opposition, right to limitation of treatment, right to portability of data and the right not to be the subject of an automated individual decision (including profiling). In particular, the Data Controller shall correct, delete, block or otherwise process the Personal Data and take any other measures in relation to Data Subjects' Requests in relation to their rights under applicable laws only in accordance with and subject to the written instructions of the Client.

Article 8 Personal Data Breach and Data Security Incidents

The Parties are aware that applicable law may impose a duty on the Client to inform the competent Supervisory Authority and the Data Subject in the event of Personal Data Breach. Such incidents must therefore be notified to the Client, regardless of their origin.

The Data Processor shall promptly notify the Client of any technical, organisational or other incidents (including incidents at Sub-processors), which have resulted or may result in a Personal Data Breach in the sense of Article 33 of the GDPR affecting Personal Data ("**Data Security Incident**"). Data Security Incident include in particular the following, without being limited to:

- (i) any actual or suspected unauthorised access, disclosure, loss, download, theft, blocking, encryption or deletion by malware or other unauthorised action in relation to Personal Data by unauthorised third parties;

- (ii) any actual or suspected operational incidents which have an impact on the Processing of Personal Data;
- (iii) any actual or suspected breach of this DPA or applicable law by the Data Processor, its employees or agents to the extent that such breach affects the integrity and security of Personal Data or materially adversely impacts the Data Processors' obligations under this DPA; or
- (iv) any legally binding request for disclosure or seizure of Personal Data by a law enforcement or other public authority unless the Data Processor is prohibited by statutory law to notify such incident to the Client.

The Data Processor shall promptly notify Data Security Incident in writing and within a maximum of forty-eight (48) hours to the Client. This notification shall be accompanied by all relevant and comprehensive documentation under applicable laws to enable the Data Controller, if necessary, to notify that Breach to the competent Supervisory Authority. Further information may be requested at a later stage as information becomes available.

The Data Processor shall assist the Data Controller, upon its first request, to perform all such actions necessary to comply with the GDPR in case of Personal Data Breach, including notification requirements. In the event of Personal Data Breach attributable to the Data Processor, the latter shall provide assistance without any additional remuneration.

In the event of Data Security Incident, the Data Processor must, with the approval of the Data Controller take appropriate measures to secure non-impacted Personal Data, mitigate possible adverse consequences for Data Subjects affected or potentially affected and put in place measures to prevent any potential Data Security Incident in the future.

In the event of breach of this DPA, the Data Processor shall be liable for any damage resulting from it and for any damages resulting from the engagement of Sub-Processor.

In the event that the Data Processor is required under applicable law to notify a Data Security Incident to a Supervisory Authority, the Data Subjects concerned or any other third parties (e.g. if the Data Security Incident results in a Personal Data Breach for which the Data Processor is itself responsible as controller), the Parties shall use their best efforts to agree on a joint approach with a view to avoid any contradiction or inconsistent information. This includes providing each other with the details of supportive documentation in the appropriate timeframe.

Article 9 Obligation of assistance by the Data Processor

The Data Processor shall maintain a written record of all categories of processing activities carried out on behalf of a Client in accordance with article 30 of the GDPR.

The Data Processor shall assist the Data Controller in any relevant matter, and notably in carrying out Data Protection Impact Assessments (“**DPIA**”) in relation to the DPA and in relation to any requests or consultations with the Supervisory Authority.

To the extent permitted under applicable law, the Data Processor shall immediately inform the Data Controller of any request, order or proceeding issued by a Supervisory Authority (National Data Protection Commission)

or any other public authority (Courts, police, etc.) concerning the processing of the Personal Data performed directly or through its Sub-Processors.

Unless provided otherwise by applicable laws and regulations, the Data Processor shall not communicate information about the Processing of the Personal Data with the Supervisory Authority or any other public authority (including regulatory authority), without the express prior consent of the Data Controller.

The Parties shall use best efforts to support each other in the event of any audits, enquiries, investigations or other proceedings initiated by a Supervisory Authority or any other public body in relation to the Processing of the Personal Data.

Article 10 Return and deletion of the Personal Data

In line with the purposes limitation principle as described in the GDPR and when no longer necessary for the purposes described in the Agreement, the Data Processor shall at the discretion of the Data Controller (i) return the Personal Data and the Processing results in a structured, commonly used, machine readable and interoperable format to the Data Controller and/or (ii) must ensure, subject to prior consent of the Data Controller, that the Personal Data, including existing copies, are securely and effectively destroyed/erased, unless the Data Processor can demonstrate there is a legal or regulatory obligation which requires it to retain all or part of the Personal Data for a longer period.

Upon completion, the return and/or destruction of the Personal Data shall be confirmed by the Data Processor to the Data Controller in writing in a reasonably detailed manner.

Article 11 Controlling rights of the Data Controller

The Data Processor shall provide within reasonable delay the Data Controller with the necessary documentation to demonstrate compliance with all its obligations with this DPA, and shall allow for and contribute to audits in relation to the Processing of Personal Data.

The Data Processor authorizes the Data Controller to conduct inspections of its data-processing facilities or audits to inspect, control or examine the Processing of Personal Data with a twenty (20) calendar days' prior written notice. Upon request of the Data Controller, the audits may be conducted by electronic means (for example a virtual data room). The Data Processor undertakes to give access to all information and documentation related to the protection of Personal Data, including notably the data processing register, the stored data and the data processing programs necessary to carry out such controls, inspections and verifications. Such audit will be carried out by either by the Data Controller or by its representatives, consultant or auditor duly mandated.

The Data Processor undertakes to cooperate and contribute in the most efficient manner to such audits. If the conduct of the audit is motivated by a breach of its obligations by the Data Processor or if the Data Controller has reasonable grounds specified in writing, to suspect a violation of its obligations by the Data Processor, the costs of such audit shall be borne by the Data Processor.

Article 12 Retention Period of the Personal Data of the Parties' employees, agent and Sub-Processors:

Each Party undertakes (i) to keep the Personal Data concerning their respective employees, agents and Sub-Processors that could have been transmitted during the preparation and execution of the Agreement, until the

expiry of the statutory limitation period in force under applicable law and (ii) to delete such Data upon expiry of this retention period.

Article 13 Transfer of Personal Data outside the European Union

The Data Processor is not authorized to transfer the Personal Data to a country outside the territory of European Union, nor to any international organisation (i) unless the Client has given its prior written consent and (ii) on condition that the Data Processor has provided appropriate safeguards to ensure an adequate level of data protection in accordance with articles 44 to 49 of the GDPR.

“Restricted Transfer” means any transfer of the Personal Data by the Data Processor or a Sub-Processor which would be prohibited by applicable law in the absence of the instruments or undertakings referred to in this article 13. Shall be considered as a Restricted Transfer any processing, operation or practice performed or initiated on the Personal Data towards a country outside the territory of the European Union.

The Data Processor will immediately upon consent given by the Client and prior to commencement of any Restricted Transfer (i) enter into the standard clauses set forth in the Commission Decision dated February 5, 2010 (2010/87/EU) and/or (ii) enter into or establish any other appropriate instruments or undertakings to comply by applicable law. The Data Processor shall enter into such instruments or undertakings with the Sub-Processor.

A copy of such safeguards may be obtained by the Data Subject by a simple request sent to the Data Controller’s DPO.

Article 14 Miscellaneous

In the event of any conflict or inconsistency between this DPA and the Agreement, the provisions of this DPA shall take precedence over the Agreement in relation to data processing only. Otherwise, the provisions of the Agreement shall remain in full force.

Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties’ intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Annexe II of contract: Offer from the Service Provider for the ELU_2025_003 Asset Connectivity API solution tender

[annex to be added]