JOINT CONTROLLER AGREEMENT
Whistleblowing System
Pursuant to art. 26 of European Regulation 679/2016 – GDPR
****

Effective date: September 26th, 2024

SIA Vendon (registration No. 40103422387)) with registered office in Ojāra Vācieša iela 6B, Rīga, LV-1004, Latvia, e-mail: cogesspa@pec.it, represented by JUAN JESUS ALBERDI LANDA

And

AZKOYEN, SA (c.F. A31065618 P. IVA: ESA31065618 with registered office at Calle del Pol. Ind. Berroa, 19, 4ª Planta 31192 Tajonar, (Navarra) Spain, represented by JUAN JOSÉ SUÁREZ.

(hereinafter, both parties will be jointly identified as "Joint Controllers" or "Parties")

WHEREAS,

1) SIA Vendon is part of the Azkoyen Group, of which the parent company is AZKOYEN, SA;
2) the Parties intend to share resources for the receipt and management of Whistleblowing reports (hereinafter also WB) through the use of a single platform and common IT systems.
   By using these common procedures, Group Companies ensure that violations of law committed by Group employees are investigated, remedied and sanctioned according to uniformly applicable standards. Each Group Company is individually responsible for prosecuting and sanctioning violations committed by Group employees identified through the procedures that make up the WB Management System;
3) Pursuant to art. 26(1) of the GDPR, joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR;
4) Article 4(1)(7) of the GDPR defines a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data";
5) it is, therefore, the intention of the Parties to regulate in a transparent manner the reciprocal rights and obligations as they result from the timely compliance with the rules and principles contained in the GDPR, as well as with the relevant national regulations, with particular regard to the exercise of the rights of the data subject, as well as the respective roles assumed in the shared management of the WB channel, arriving at the signing of this agreement;

IT IS AGREED AND STIPULATED AS FOLLOWS

Article 1 – Preliminary agreements

1. Within the scope of their respective responsibilities as determined by this Agreement, the Joint Controllers shall at all times fulfil their obligations in accordance with it and in such a way as to process the data without violating the provisions of the law in force on the subject and in full compliance with the guidelines provided by Anac.

2. It is understood between the Parties that, pursuant to art. 26, paragraph 3, of Regulation (EU) 2016/679, regardless of the provisions of this Agreement, the data subject may exercise his/her rights against and against each Joint Data Controller.

3. In line with their mission and values, the Joint Controllers mutually undertake to process and protect the personal data of any natural person who may come into contact with or work with them ("Data Subject"), respecting the

identity, dignity of every human being and the fundamental freedoms constitutionally guaranteed in compliance with the GDPR relating to the protection of natural persons with regard to the processing of personal data and free movement of the same.

6. Any modification or addition to this agreement may only be made in writing, under penalty of nullity.

7. The essential content of this Joint Controller Agreement is made available to the Data Subject by each of the Joint Controllers.

Article 2 - Object of the processing

The joint controllership extends to every operation carried out as part of the Whistleblowing System and permeates every aspect of its organization within the Group.

Jointly, the parties hereby intend to share resources for the reception and management of whistleblowing reports. In particular, the parties share the following resources:

(a) whistleblowing handlers;

b) whistleblowing platform;

c) reporting channel for the receipt of paper mail.

AZKOYEN, SA plays a central role in the Whistleblowing Management System, providing the technical and organizational infrastructure necessary for the effective conduct of the procedures that make up the Whistleblowing System.

All reports (with the exception of the request for a face-to-face interview) will be processed by the person appointed by AZKOYEN, SA, who is obliged to inform the person responsible for reporting at local level, such as the CEO of SIA Vendon, of the transmission of a report (limiting itself to reporting the information that can be communicated by law).

The parent company AZKOYEN, SA is still responsible for the management and storage of the documentation relating to the report.

Following the conclusion of the process of ascertaining the facts reported, the parties, through the persons specifically authorized and appointed, will share information with each other regarding the results obtained and, where necessary, will agree on the consequent measures to be taken.

The Joint Controllers declare, with regard to the processing of Personal Data, that they share the decisions relating to the purposes and methods of data processing and, in particular:

- the purposes of the processing of personal data, each with its own specificities related to the activities actually carried out;

- the means of processing and the methods of processing personal data;

- the data retention policy;

- the style and methods of communication of the information art. 13 and 14 of the GDPR;

- the procedure for managing consents (where necessary);

- the designation and training of authorised persons;

- the management of communications and appointments of data processors pursuant to art. 28 of the GDPR;

- the keeping of records of the processing pursuant to art. 30 of the GDPR;

- the tools and means used for the implementation of decisions and, in part, also for the operations of the Joint Controllers, especially in relation to physical, organisational and technical security measures;

- the risk-based approach;

- the profiles and the personal data security policy, the Data Breach procedure and the Personal Data Protection Impact Assessment (DPIA) procedure;

- the management of the procedure for exercising the rights of the Data Subject;

The Joint Controllers agree that the personal data acquired during the management of any report will be processed for the sole purpose of processing the report received.

Article 3 – Duration and effects resulting from the termination of the Contract

1. This Agreement shall become effective between the parties immediately upon its signing and shall be valid indefinitely, unless amendments are made to be approved in writing. Each Party may terminate the Agreement unilaterally by notifying the other Party at least 30 days in advance.

2. The processing of personal data under the joint controller regime will, in any case, have a duration not exceeding that necessary for the purposes for which the personal data were collected and such data must be adequately stored in the systems and databases of the joint controller company AZKOYEN, SA in a form that allows the identification of the Data Subjects for a period of time not exceeding that allowed by current legislation.

3. Following the cessation of the processing, the Joint Controllers will be required to provide for the complete destruction of the personal data processed, except only in cases where the storage of the data is required by law and/or other purposes or in the event of autonomous and additional circumstances that justify the continuation of the data processing by the individual Joint Controllers, in a limited manner and for the period of time strictly necessary for this.

Article 4 – Obligations between the parties

1. The protection of personal data is based on compliance with the principles illustrated in this document that the Joint Data Controllers undertake to disseminate, respect and ensure that their directors, employees and collaborators and third parties with whom they collaborate in the performance of their activities comply. In particular, the Joint Controllers are committed to ensuring that the personal data protection policy, and all that follows from it, is understood, implemented and supported by all parties, internal and external, involved in the activities of the Joint Controllers, taking into account their concrete reality, their possibilities, including economic ones, and their values.

2. The Joint Controllers undertake to maintain and guarantee the confidentiality and protection of the personal data collected, processed and used by virtue of the joint controllership relationship. In particular, they undertake, even separately, to:

a) communicate and disseminate its policy regarding the protection of personal data;

b) process personal data in a lawful, fair and transparent manner in line with the constitutional principles and current legislation on the subject, in particular the GDPR, and only for the time strictly necessary for the purposes envisaged, including those to comply with legal obligations;

c) collect personal data limited to those that are indispensable to carry out the activities covered by this agreement;

d) process personal data according to the principles of transparency for the specific purposes expressed in its own policies;

f) adopt processes for updating and correcting the personal data processed to ensure that the personal data are, as far as possible, correct and up-to-date;

g) store and protect the personal data in its possession with the best available preservation techniques;

h) ensure that personal data protection measures are continuously updated. This commitment will be constantly followed within the framework of the principle of accountability by constantly implementing appropriate technical and organizational measures and appropriate policies, to guarantee and be able to demonstrate that the processing is carried out in accordance with the GDPR taking into account the state of the art, the nature of the personal data stored and the risks to which they are exposed. Each Joint Controller will periodically monitor the level of security achieved, in order to ensure that it is always appropriate to the risk;

(i) ensure the timely recovery of the availability of personal data in the event of a physical or technical incident

(l) to make clear, transparent and relevant the manner in which personal data is processed and stored in such a way as to ensure adequate security;

m) foster the development of a sense of responsibility and awareness of the entire organization towards personal data, seen as data owned by the individual data subjects;

n) ensure compliance with the laws and regulations applicable to the protection of personal data, possibly updating the management of the protection of personal data;

o) prevent and minimise, to the extent available to the extent available, the impact of potential breaches or unlawful and/or harmful processing of personal data;

p) promote the inclusion of personal data protection in the continuous improvement plan that the Joint Data Controller pursues with its management systems.

3. The Joint Data Controllers undertake, with particular regard to the exercise of the rights of the Data Subject and their respective functions of communicating the information referred to in Articles 13 and 14 of the GDPR, to standardise the methods, style, models and, above all, the procedures for the protection of personal data in favour of the Data Subject.

4. The communication of the personal data necessary to ensure the pursuit of the common project will take care of their accuracy, truthfulness, updating, relevance and not exceeding the purposes for which they were collected and will be subsequently processed.

Article 5 - Persons authorised to process (and Designated)

1. Each of the Joint Controllers shall identify and designate the persons authorised to carry out processing operations on the data processed in pursuit of the shared purpose and provide for the relevant training, including on the principles of lawfulness and fairness to which this policy for the protection of personal data and the processing of personal data must comply as well as compliance with the safeguard measures adopted.

2. Each of the Joint Controllers guarantees that its employees and collaborators involved in the whistleblowing process are reliable and have full knowledge of primary and secondary legislation on the protection of personal data.

3. Each of the Joint Controllers shall identify a contact person within its structure, with the task of liaising with a similar person designated by the other party, to oversee the correct fulfilment of the provisions of this agreement. The name and contact details of the internal contact person shall be promptly communicated to the other party.

Article 6 - Data Processors

1. Any of the Joint Controllers that deems it necessary to make use of a data processor for the performance of specific activities required under the joint project shall notify the other party with adequate notice.

2. Specific data protection obligations shall be imposed on that controller by means of a contract or other legal act under Union or Member State law, in particular by providing for sufficient safeguards to put in place appropriate technical and organisational measures in such a way that the processing meets the requirements of applicable law.

3. The relationship between the Joint Controllers and any data processors shall remain governed by Article 28 of the GDPR.

Article 7 – Impact Assessment and Personal Data Violations

1.The impact assessment on the protection of personal data and its possible review, are the responsibility of the Azkoyen Group (Azkoyen S.A.), in the person of the IT Director Luis Villafranca Rodriguez, who promptly informs the other Joint Controller of the relevant need and of the activity carried out.

2. In the event of a breach of the security of personal data resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and likely to jeopardise the rights and freedoms of the individuals whose personal data are processed in the context of the Joint Project, the coordination activity for the purpose of fulfilling the obligations referred to in Articles 33 and 34 of the GDPR is entrusted to Azkoyen Group (Azkoyen S.A.), in the person of the IT Director, who will take care of the preparation of a specific document (*Data Breach Policy*), if not already existing and adopted.

3. In the event of a personal data breach, the Joint Controller who is not assigned the coordination activity shall:

a) to inform the other Joint Data Controller promptly and in any case no later than 24 hours after the discovery of the event, by email, that it has become aware of a breach by providing it with all the details of the breach suffered, in particular a description of the nature of the personal data breach, the categories and the approximate number of data subjects involved, as well as the categories and approximate number of records of the data in question, the impact of the personal data breach on the Data Subjects involved, and the measures taken to mitigate the risks;

b) provide assistance to deal with the violation and its consequences, especially for the Data Subjects involved. It will also take action to mitigate the effects of violations, proposing timely corrective actions and implementing all corrective actions approved and/or requested by the Joint Controller assigned to the coordination activity. These measures are required to ensure a level of security appropriate to the risk related to the Processing performed.

4. Each Joint Controller undertakes to prepare and maintain an internal register of personal data breaches and to collect and store all documents relating to each breach, including those relating to the circumstances relating to it, its consequences and the measures taken to remedy them.

Article 8 - Decisions on international transfers of personal data

1. This agreement provides that personal data will be processed exclusively within the territory of the European Union.

Article 9 - Sharing of the procedure for the exercise of the rights of the Data Subject

1. The Joint Controllers designate a unitary internal contact person as a point of contact for the interested parties, identified in the figure of the IT Security Manager of Azkoyen S.A., in the person of the Azkoyen Group IT Director.

2. Requests to exercise rights and any complaints submitted by data subjects will be handled exclusively by the Information Security Manager of Azkoyen S.A., who can be contacted at the addresses that will be disclosed together with his name within the specific information provided by the Joint Data Controllers, it being understood in any case that the data subjects may exercise their rights against each Joint Data Controller.

2. In particular, if the contact person receives requests from the Data Subject, aimed at exercising his/her rights, he/she shall:

- promptly notify each Joint Data Controller in writing by email;

- coordinate, where necessary and within its competence, with the internal functions designated by each Joint Data Controller to manage relations with the Data Subject;

- verify the existence of the conditions and allow, defer or refuse their exercise, giving timely written notice to each Joint Data Controller via e-mail.

3. The contact persons identified by the Parties shall also provide assistance to each of the Joint Controllers in the context of administrative and judicial proceedings initiated by the Data Subject or by the Supervisory Authority as a result of the activity referred to in this article.

Article 10 - Verification of compliance with the rules for the protection of personal data

1. Each of the Joint Controllers shall recognise the right of the other to carry out audits in relation to the operations concerning the processing of personal data in the context of the Joint Project. To this end, each of the Joint Data Controllers has the right to order – at its own care and expense – sample checks or specific audit or reporting activities in the field of personal data protection and security, making use of personnel expressly appointed for this purpose, at the premises of the other, with the sole and untouchable limit of the protection of the privacy of the data subject that the specific purpose of shared processing requires.

2. Each of the Joint Controllers shall make available all documentation necessary to demonstrate compliance with all its obligations and to enable audits, including inspections, to be conducted and to contribute to such verifications.

3. Each of the Joint Controllers must promptly inform and involve the other party in all matters concerning the processing of personal data and in particular in the case of requests for information, controls, inspections and access by the Supervisory Authority.

Article 11 - Liability for breach of provisions

The Joint Controllers undertake, jointly and severally, to prepare, implement and keep up to date all the obligations required for the protection of personal data.

Article 12 - Data Protection Officer

1. Each of the Joint Data Controllers informs that it has, if necessary, appointed the Data Protection Officer (DPO) in accordance with the provision contained in art. 37, par. 1, letter a) of the GDPR, identifying, as a suitable subject:

Data Protection Officer and that the same can be reached at the following addresses:

Telefono: +34 948709872 - E-mail: responsableseguridad@Azkoyen.com

Article 13 – Communications

Any communication relating to this agreement must be given in writing and by email, with acknowledgement of acceptance and confirmation of delivery, provided that they are sent or delivered to the address indicated at the top of the agreement. This address may be changed by either of the Parties, giving notice to the other in accordance with this article.

Article 14 – Final provisions

For anything not expressly indicated in this Appendix, the GDPR, the provisions of the law in force, as well as the provisions of the Supervisory Authority shall be applied.

SIA Vendon	Azkoyen S.A.
JUAN JESUS ALBERDI LANDA	JUAN JOSÉ SUÁREZ
Legal representative Vendon SIA	Azkoyen Group CEO