



AZKOYEN.
GROUP

WHISTLEBLOWER CHANNEL POLICY

AZKOYEN GROUP



- **Versions control**

| Version | Date | Author | Changes made |
|---------|----------------|--------------|-----------------|
| 1.0 | September 2019 | Support unit | Initial release |

- **Approvals**

| Governing body | Entity | Date | Signature |
|--------------------|-------------------|----------------|-----------|
| Board of Directors | GRUPO AZKOYEN, SA | September 2019 | |



| | |
|---|----|
| 1. Introduction to the Whistleblower Channel | 4 |
| 2. Subjective scope | 4 |
| 2.1 Who should make a report through the Whistleblower Channel? | 5 |
| 2.2 Who can be the subject of a report via the Whistleblower Channel? | 5 |
| 3. Objective scope | 5 |
| 4. Means of receiving reports. How should reports be made? | 6 |
| 5. Safeguards for the complainant | 7 |
| 5.1 Prohibition against retaliation | 7 |
| 5.2 Confidentiality regarding the identity of the complainant | 8 |
| 5.3 Measures in situations of conflict of interest | 8 |
| 6. Procedure for processing reports | 9 |
| 6.1 Receipt of reports | 9 |
| 6.2 Investigation of the events reported | 10 |
| 6.3 Proposed decision | 10 |
| 6.4. Application of the sanction | 11 |
| 7. Protection of personal data | 11 |
| 7.1. Information clause on personal data protection | 11 |
| 7.2. Principle of proportionality | 12 |
| 7.3. Security and confidentiality measures | 12 |
| ANNEX I | 13 |
| Behaviour that may be reported via the Whistleblower Channel | 13 |
| ANNEX II | 17 |
| Report form | 17 |



1. Introduction to the Whistleblower Channel

AZKOYEN Group's prestige and reputation, as well as the leading role it occupies, are the results of many years of hard work and effort by each and every member of the Company. However, inappropriate behaviour by even a single employee can damage our image and reputation at any time. For this reason, the AZKOYEN Group actively works to prevent and avoid such eventualities.

Thus, and among other issues, all employees and collaborators acting on behalf of AZKOYEN are required to act in accordance with and respect at all times (i) current legislation, (ii) the Code of Conduct and (iii) internal policies and procedures. As part of this prevention effort, it is of great importance that all employees cooperate in detecting inappropriate behaviour.

In this regard, the current legislation (*and especially the current Spanish Criminal Code, following the reforms of 2010 and 2015, and Circular 1/2016, of 22 January issued by the Spanish Attorney General's Office*) reinforces the need for companies to have “**criminal risk prevention models**”, which is a control systems and mechanisms making it possible to prevent, detect and react to the risk of a crime being committed in a company, and for its benefit, by any person in the company.

The so-called “Whistleblower Channel” plays a fundamental role in the effectiveness of these prevention models. This channel, in line with the ethical and compliance culture at AZKOYEN, allows all company staff to report possible risks or breaches.

In light of the above, this Policy describes all issues relating to the operation of the AZKOYEN Whistleblower Channel: Who can make a report, against whom, in what circumstances and, above all, what steps are followed when a report is received. Naturally, all of these steps are subject to absolute confidentiality which is a fundamental pillar of the channel.

In this way, all Azkoyen personnel should be familiar with this tool which is, without doubt, of great value and utility to help us all to preserve and protect the Group's image, prestige and reputation.

2. Subjective scope

The Whistleblower Channel is aimed at all of the staff (as listed below) of all the companies that make up AZKOYEN, who are or may be aware of an irregularity committed by any other worker, manager or director.



2.1 Who should make a report through the Whistleblower Channel?

All (i) employees, (ii) executives (understood as those who provide management services to the company and have powers of representation, organisation or control in it, regardless of whether their contractual relationship with AZKOYEN is labour or commercial), (iii) the members of its Board of Directors *as well as (iv) its external collaborators (agents, subcontractors or other third parties acting under the authority of AZKOYEN)*, (v) all clients and suppliers of the Azkoyen Group; should report, via the Whistleblower Channel, any irregularity that they are aware of and that is included in its objective scope, without fear of being the subject to dismissal or any other form of retaliation, and with the certainty that their report will be treated with the utmost confidentiality.

The aforementioned groups and/or categories of people are referred to hereinafter, jointly and indistinctly and for the exclusive purposes of this document, as the "**staff**".

In this regard, please note that AZKOYEN Group refers to all of its component commercial companies, which are listed on our website <http://www.azkoyen.com/quienes-somos>, and whose parent company is "GRUPO AZKOYEN, SA" (for the purposes of this document they are referred to as the "**Group**").

2.2 Who can be the subject of a report via the Whistleblower Channel?

All employees, executives, members of the Board of Directors or external collaborators of the Group subject to its authority who have committed any form of irregularity or inappropriate behaviour as listed in the objective scope of this document may be subject to report.

3. Objective scope

The behaviours that can be reported via the Channel (hereinafter, "**the objective scope**") are those detailed in **Annex I** and listed below. These behaviours are criminal offences under the Spanish Criminal Code (or in other specific laws) and could result in liability for the Group:

- Public corruption
- Business corruption
- Fraud
- Misleading advertising
- Money laundering / Terrorist financing
- Smuggling



- Bankruptcy fraud
- Thwarting implementation
- Computer damages
- Crimes related to intellectual and industrial property
- Disclosure of company secrets
- Offences against personal and family privacy
- Public finance fraud
- Non-compliance with accounting obligations
- Social security fraud
- Subsidy fraud / Fraud against the EU budget
- Crimes against natural resources or the environment
- Offences relating to risks caused by explosives or other substances
- Financial market offences
- Offences against the rights of foreign citizens
- Crimes against public health
- Price fixing
- Fraudulent billing
- Counterfeiting of legal tender or securities
- Alteration of prices in public tenders and auctions
- Offences against workers' rights
- Refusing inspection

Additionally, all those behaviours that are contrary to the principles and rules of behaviour set out in the AZKOYEN Group Code of Conduct may also be reported via the Whistleblower Channel.

4. Means of receiving reports. How should reports be made?

In principle, and with certain exceptions indicated below, all the reports that are to be made must be submitted to the "Support Unit" of the Audit Committee¹.

Reports must be made and submitted in writing. The complainant may choose any of the channels provided for this purpose:

- Via the corporate intranet, at the following section or link: www.azkoyen.com/responsabilidad-social-corporativa/

¹ The **Audit Committee** (*appointed by the Board of Directors to supervise the proper functioning of the AZKOYEN Compliance model*) has delegated the function and responsibility to manage and investigate all reports received to the Support Unit.

The Support Unit currently consists of the Azkoyen Director of Human Resources who may also draw on expert legal advice regarding the various matters that may arise.



- By post, addressed to the attention of the "Support Unit of the Audit Committee", Avenida San Silvestre, s/n, postcode: 31350, Peralta, Navarra, Spain.

In both cases, the complainant must use the report form (Annex II). It is available on the corporate intranet at the section mentioned above. Where reports are sent by post, the form must be downloaded and duly completed.

Due to its importance, it is expressly stated that any report not made via the means above may be deemed as not received or admitted for processing. In such cases, the report will be deleted and destroyed.

Complainants must identify themselves when making the report. Anonymous reports will not be accepted. However, throughout the procedure the complainant's identity will be kept confidential, thus complying with the privacy requirements established, among others, by the Spanish Organic Law on Data Protection and by the Spanish Agency for Data Protection.

Privacy is one of the most important issues with regard to the operation of the Channel. Precisely for this reason anyone, including AZKOYEN external collaborators, who may have a role at any time in a possible report, will be subject to the most absolute obligation of confidentiality and professional secrecy.

5. Safeguards for the complainant

5.1 Prohibition against retaliation

Anyone making any kind of report in good faith as provided herein is protected against any type of retaliation, discrimination or penalisation as a result of filing a report. AZKOYEN will sanction any type of retaliation against any good faith complainant, understanding retaliation, among others and by way of example, as dismissal, unjustified reduction of any bonus, transfer to another site, or the assignment of lower-ranking functions and responsibilities.

Any complainant who feels they have been the victim of retaliation as a result exclusively of having filed a report may inform the Support Unit, which will study the case and take appropriate steps to prevent the retaliation or, failing that, to correct it.

The prohibition of retaliation provided for in the preceding paragraphs shall not prevent the adoption of justified disciplinary measures where an internal investigation determines that a report is false and that the person who made it was aware of its falsity and thus acted in bad faith.²

² In this regard and in accordance with the provisions of article 456 and thereafter of the Spanish Criminal Code, it is expressly stated that false accusations or reports and the simulation of offences are considered a crime punishable by up to two years in prison.

5.2 Confidentiality regarding the identity of the complainant

AZKOYEN guarantees maximum confidentiality regarding the identity of the complainant.

As a measure to guarantee this confidentiality, it is expressly stated that the right of access by the person accused in the report, as provided for in Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data, does not include the identity of the complainant. Consequently, and unless there is a judicial ruling to the contrary, AZKOYEN does not provide the accused person with the identity of the complainant.

This principle of confidentiality is one of the basic pillars of the Whistleblower Channel, whose correct operation depends on being able to guarantee whistleblowers that their identities will be protected, so as not to discourage whistleblowing.

Likewise, both the Support Unit and the Audit Committee are obliged to uphold professional secrecy regarding the identity of the complainant. If exceptionally, an external advisor or another member of AZKOYEN takes part in the investigation of the facts, they would be subject to the same obligation of confidentiality and professional secrecy.

5.3 Measures in situations of conflict of interest

In the event that the facts reported pertain to the functions of the Support Unit, or those of any of the members of the Audit Committee, or may generate a conflict of interest in any way for any of these people, the affected person must refrain from participating in the reports processing procedure, as described below.

A conflict of interest will be deemed to exist in cases where the private interests of any of these people may constrain their ability to carry out the processing and investigation of reports with due objectivity, neutrality and impartiality. Such a conflict is presumed to exist when the events reported fall within the responsibilities and executive functions of any of the members of the Audit Committee or the Support Unit, and may also arise when the events affect someone with whom any of them have family ties (up to third grade, inclusive) or business interests (holding more than 10% of the shares or stock in the same company).

As a consequence of the above, if the complainant suspects that the facts could imply a conflict of interest with the Support Unit, they may submit the report directly to the Audit Committee or to the secretary of the Board of Directors if the conflict of interest affects any of the members of the Audit Committee. In such cases, and if the existence of such a conflict of interest is confirmed, an external expert will be entrusted with the processing and investigation of the report, not having to follow the budgetary management controls that may apply for contracting.

6. Procedure for processing reports

6.1 Receipt of reports

Except for the assumptions set out in section 5.3 above, all reports that are made will be received by the Support Unit, which will deal with their receipt, and will carry out a preliminary analysis of the events reported and the use of the form provided. After that, it will decide whether to launch the corresponding investigation or reject the report as inadmissible, as provided in this Policy, within a maximum of five (5) business days, counting from its effective receipt.

- a) **Inadmissibility of a report:** if the report does not comply with the formal requirements established herein, or it is evident that the facts reported do not constitute one of the infringements provided for in the objective scope of the Whistleblower Channel, the Support Unit will reject it as inadmissible.

After this, and within a non-extendable period of two (2) business days, the Support Unit will notify its decision to the Audit Committee, which, if there are reasons that justify it may, exceptionally, overturn the decision and require that the Support Unit admit the report for processing. For this, the Committee will have ten (10) business days, counting from the receipt by its secretary of the Support Unit's decision.

- b) **Admission of a report for processing and launch of the investigation phase:** When a report made complies with the formalities and, in addition, the facts reported are within the objective scope of the Whistleblower Channel, there being indications that they have taken place, the Support Unit will agree to admit it for processing.

After following the above steps and deadlines, the decision adopted by the Support Unit in this phase of the procedure will be communicated to the complainant within a maximum period of five (5) business days, unless a longer period is necessary for justified causes.

Likewise, any person who has been the subject of a report admitted will be informed about **(i)** the receipt of the report, **(ii)** the facts reported against them, **(iii)** the departments and third parties that, where appropriate, may receive the report, and **(iv)** how to exercise his rights of access, rectification, deletion and opposition, in accordance with data protection regulations.

However, the right of access of the accused will be limited to their own personal data being processed, which is why, and given the confidential nature of reports, the accused will not be entitled to know the identity of the complainant or their personal data.

Exceptionally, if the Support Unit considers that there is a risk that notifying the accused will compromise the investigation, the notification may be deferred until this risk disappears. In any event, the deadline to notify the accused may not exceed one (1) month from the date the report has been received, with the possibility of extending

this deadline to a maximum of three (3) months if there are justified grounds. All without prejudice to the fact that the law may expressly establish other, mandatory deadlines, in which case these deadlines must apply.

6.2 Investigation of the events reported

Once the report is admitted, the Support Unit will launch the appropriate investigations to verify the veracity of the events reported. To do so, it may request as much information and documentation as it deems necessary to try to clarify the events reported.

For their part, and whenever requested, AZKOYEN staff must cooperate fully with the investigation.

In the event that, due to the nature of the events, the investigation is likely to be complex, then specialised support or advice may be sought from an external expert, who will coordinate with the Support Unit and the Audit Committee.

6.3 Proposed decision

Once the investigation is concluded, two further steps will be taken:

- First, the Support Unit will notify the results to the Audit Committee and will propose (i) to close the report or a (ii) decision.
- Once this is done, and in light of said report, the Audit Committee will adopt the decision that, in its opinion, is appropriate.

In this sense, the Audit Committee will agree to close the report and the actions carried out if there is insufficient evidence to support the events reported, or if they do not constitute an infringement included in the objective scope of the Whistleblower Channel.

On the contrary, if the Audit Committee considers that there is sufficient evidence of the events reported and, furthermore, they constitute an infringement included in the objective scope of the Whistleblower Channel, it will issue a reasoned decision indicating the legal steps, of whatever nature, to be taken. When issuing its decision, the Audit Committee will not be bound by the proposal made by the Support Unit but will have full freedom and sovereignty to take whatever decision it deems most appropriate, in each case.

At any point in the procedure, the Audit Committee may also call on an external subcontracted expert for advice and legal assistance, for example, regarding aspects such as drafting a statement of the facts, their classification, or the adoption of the most appropriate disciplinary measures in each case.

In the event of a conflict of interest situation, in the terms set out in section 5.3 above, the final decision will be taken jointly by the Chairman and the Secretary of the Board of Directors.

6.4. Application of the sanction

Application of the sanction or disciplinary measures agreed, in each case, will fall to the person or persons holding said functions and duly empowered.

The Director of Human Resources will be responsible for applying any employment-related sanctions. If the sanction is of a commercial nature (contractual termination, etc.) or requires the Audit Committee to take legal action, the sanction will be carried out by someone who is sufficiently empowered.

7. Protection of personal data

In designing this Channel, AZKOYEN has fully complied with the applicable regulations on data protection; in particular Spanish Organic Law 15/1999, of 13 December, on the Protection of Personal Data ("LOPD") and its implementing regulations. Likewise, the Whistleblower Channel has been designed in accordance with the Spanish Agency for Data Protection Legal Report 0128/2007 entitled "Creation of internal reporting systems in companies ("*Whistleblowing*" mechanisms)", and with "Report 1/2006 on the application of the data protection rules of the European Union to internal "*Whistleblowing*" mechanisms in the field of accounting and internal audit controls, the fight against fraud and banking and financial crimes", of the Article 29 Working Group of the European Commission.

7.1. Information clause on personal data protection

The personal data collected in the context of the Whistleblower Channel will be handled with the sole purpose of processing the reports received and, if appropriate, investigating the reality of the events reported, thus complying with the requirements laid down in Spanish Organic Law 1 / 2015, of 30 March, and in Spanish Organic Law 15/1999, of 13 December, on the Protection of Personal Data.

Those data that are collected in the context of a report and that give rise to a corresponding investigation will be included in the file "Whistleblower Channel", which will be duly declared to the Spanish Agency for Data Protection. The data controller for the file is GRUPO AZKOYEN, SA with Tax ID No. A-31065618, and registered office at Avenida San Silvestre s/n, 31350, Peralta, Navarra (Spain)

On the other hand, it is expressly stated that the data contained in any report that are not admitted for processing will not be included in any file but instead eliminated.

Both the complainant and the accused will be duly informed, in both eventualities, of the specific persons and bodies to whom their data will be communicated, in accordance with the provisions of this policy, especially as regards the possible non-notification of the accused of the complainant's identity.



To revoke consent after it is granted, as well as to exercise the rights of access, rectification, deletion, opposition, limitation, portability and the right not to be subject to automated decisions, please send a written request by post to: Avenida San Silvestre, s/n. Post code: 31350 Peralta (Navarra, Spain); or by email to: responsableeguridad@azkoyen.com.

The request should include: The name and surname of the interested party; a copy of their National Identity Document, passport or other valid identification documents of the interested party and, where appropriate, of their representative, as well as the capacity of the representative; address for notifications and the purpose of the request.

Notwithstanding the above, the accused person's right to access will be limited to their own personal data. They will not be granted access to data regarding the identity of the complainant in light of the confidential nature of the Whistleblower Channel.

7.2. Principle of proportionality

The personal data collected in the context of the Whistleblower Channel:

- ✓ Will be limited to those data strictly and objectively necessary to process the reports and, if appropriate, verify the reality of the events reported;
- ✓ They will be handled at all times in accordance with the applicable data protection regulations, for legitimate and specific purposes in relation to the investigation that may arise as a result of the report;
- ✓ They will not be used for incompatible purposes;
- ✓ They will be suitable and not excessive in relation to the aforementioned purposes.

7.3. Security and confidentiality measures

AZKOYEN will ensure that all necessary technical and organisational measures are taken to preserve the security of the data collected in order to protect it from unauthorised disclosure or access.

For these purposes, AZKOYEN has adopted appropriate measures to guarantee the confidentiality of all the data and will ensure that data relating to the identity of the complainant are not disclosed to the accused during the investigation, respecting in all cases the person's fundamental rights without prejudice to the actions that, where appropriate, may be taken by the competent judicial authorities.

ANNEX I

Behaviour that may be reported via the Whistleblower Channel

The behaviour that may be reported via the AZKOYEN Group Whistleblower Channel includes any **breach of the principles and rules of behaviour established in the Group's Code of Conduct**, which is available to all Group employees on the Employee Portal.

Likewise, any behaviour punishable under the Spanish Criminal Code or other crimes punishable under other specific laws that may lead to criminal liability for the Group, such as:

- ✓ **Bribery:** Offering or giving officials, authorities, organisations and Government Bodies a gift or compensation, financial or of another nature, with the intention of obtaining a benefit for AZKOYEN, whether legal or illegal.
- ✓ **Influence peddling:** Taking advantage of any situation arising from a personal relationship to achieve a decision that can generate, directly or indirectly, an economic benefit for AZKOYEN.
- ✓ **Business corruption:** Where a manager, administrator, employee or collaborator of AZKOYEN himself or via an intermediary, receives, requests or accepts an unjustified benefit or advantage of any kind, for himself or a third party, as consideration to improperly favour another party in the acquisition or sale of merchandise, or in the contracting of services or in business relationships. Or, conversely, the promise or concession of a favour to a third party for the acquisition or sale of products in business relationships.
- ✓ **Corruption in international transactions:** Offering or providing an unfair benefit or advantage to public officials to obtain favourable treatment in international economic activities.
- ✓ **Fraud:** Deceiving another, for profit, into carrying out an act that harms him or a third party.
- ✓ **Misleading advertising:** Marketing or advertising products or services on the basis of false claims or unclear characteristics which could therefore result in serious, evident damage to users.
- ✓ **Revealing or disclosing company secrets:** Availing oneself, by any means, of data, documents (either written or electronic), electronic storage media or any other objects containing confidential information on another company, entity, etc., with the intention to use, disseminate, disclose or transfer it.
- ✓ **Fraud involving public subsidies:** Obtaining subsidies or aid from Government Bodies in an amount or for a value greater than 120,000 Euros, falsifying documents to meet the eligibility criteria or concealing proof that would have impeded the grant from being made.



- ✓ **Public finance fraud:** Public finance fraud (national, regional, provincial or local) in an amount greater than 120,000 euros; evading the payment of taxes, withholding taxes or monies that should have been withheld to pay taxes, or income on account of remuneration in kind, or improperly obtaining returns or enjoying tax benefits in the same way.
- ✓ **Social Security fraud:** Evading paying Social Security contributions by improperly obtaining refunds or enjoying deductions.
- ✓ **Non-compliance or fraud with regard to accounting obligations** Serious failure to comply with the obligation to keep commercial accounting records and/or books. This is an offence which is usually coupled with other fraudulent behaviours as it is usually perpetrated by means of double accounting and false accounting entries.
- ✓ **Crimes against natural resources or the environment:** Directly or indirectly causing, emitting or carrying out emissions, spills, radiations, extractions, excavations, earthworks, noise, vibrations, injections or deposits, in the atmosphere, soil, subsoil or ground, underground or marine waters; creating deposits or landfills of solid or liquid waste or residues that are toxic or dangerous and can seriously harm the balance of natural ecosystems or human health.
- ✓ **Thwarting implementation:** Carrying out any act to dispose of assets or create obligations that hinder or prevent a seizure or a claim for an amount from being implemented. Hiding assets from an administrative or judicial proceeding. Using the depositary of goods seized by the authorities without proper authorisation.
- ✓ **Bankruptcy fraud:** In the hypothetical event that the company declares bankruptcy, this crime involves an act to dispose of the assets to artificially reduce the assets that guarantee the fulfilment of financial obligations, or which makes it difficult or impossible for the creditor to ascertain the debtor's true financial situation.
- ✓ **Intellectual property crimes:** Reproduction, plagiarism or public communication of all or part of a work, whether literary (book), artistic (picture or photograph) or scientific (specific theories, applications or computer programs), or its transformation, interpretation, performance or display on any medium or by any means, without the permission of the holders. This offence also covers the use of applications or computer programs without the corresponding user licence, for example.
- ✓ **Industrial property crimes:** Playing, imitating, etc. a distinctive sign without the owner's consent, so as to obtain another sign identical to or confusable with the original, applied to the same or similar products, services, activities or establishments.



- ✓ **Computer damages:** Erasing, damaging, degrading, eliminating or removing access to third parties' data, computer programs or electronic documents without authorisation and with serious consequences. Preventing or hindering the functioning of third-party computer systems.
- ✓ **Counterfeiting of legal tender or securities:** Tampering with or fabricating counterfeit currency. Importing or exporting counterfeit or altered currency. Knowingly transporting, selling or distributing counterfeit or altered currency.
- ✓ **Offences against personal and family privacy** Obtaining, using or altering private personal or family data belonging to a third party, without authorisation, contained in databases or on computer, electronic or telematic media, or in any other public or private file or register, to the detriment of said third party. Unlawfully accessing a computer system to extract personal data contained therein.
- ✓ **Offences against the rights of foreign citizens:** Promoting, favouring or facilitating illegal trafficking or immigration.
- ✓ **Money laundering:** Accepting funds, deposits, etc. that are the proceeds of criminal activity, or carrying out any other act to hide the illegal origin of the funds or to otherwise aid the person who committed the offence. This offence can be committed through negligence, i.e. as a result of a lack of due diligence. The offender need not commit the offence intentionally and knowingly.
- ✓ **Financing of terrorism:** Providing, collecting or accepting funds with the intention of using them to commit crimes related to terrorist organisations and groups.
- ✓ **Crimes against public health:** Placing products on the market that are harmful to health and/or that do not comply with legally established requirements relating to expiry or composition. Or making, shipping, supplying or trading in substances that are harmful to health.
- ✓ **Offence against workers' rights:** Seriously endangering workers' life, health or safety by infringing occupational risk prevention regulations. This offence may be committed through negligence. Using deceit or abuse of a situation of need to impose labour or Social Security conditions on workers that damage, eliminate or restrict their rights. Imposing inadequate working conditions or conditions that are contrary to occupational health and safety regulations; handling workers in a discriminatory or unequal manner; preventing or curtailing the right to freedom of association.
- ✓ **Financial market offences:** Using or supplying relevant information for the listed price of any class of financial instruments. Knowingly spreading false news or rumours about people or companies in order to alter or preserve the price of a security or financial instrument. Misrepresenting the economic/financial information contained in the prospectuses of any financial instruments.



- ✓ **Handling of toxic, corrosive and other substances:** Contravening the safety standards established for the manufacture, handling, transportation, possession or sale of explosives, flammable, corrosive, toxic or asphyxiating substances, endangering the life, physical integrity or health of people or the environment.
- ✓ **Refusing inspection:** Refusing to cooperate with the inspection authorities as regards their activities relating to companies subject to or operating in markets subject to administrative supervision.
- ✓ **Illegal financing of political parties:** Illegally giving donations or contributions to a political party, federation, coalition or electoral group.
- ✓ **Fraudulent billing:** Altering or manipulating automatic devices that measure the cost of products or services sold (meters, taximeters, etc.) with the aim of billing higher amounts, thus causing harm to consumers.
- ✓ **Smuggling:** Illegally importing or exporting goods, provided that the value of the goods, merchandise or items is equal to or greater than 150,000 euros. Otherwise violating customs regulations.
- ✓ **Altering prices in public tenders or auctions:** Requesting an advantage in order to not take part in a public tender or auction; attempting to prevent bidders from participating in a public tender or auction by means of threats, gifts, promises or any other device; colluding with another bidder in order to alter the auction price, or fraudulently renouncing a tender which has been awarded.
- ✓ **Price fixing:** Altering the prices that should be set by free competition of products or services.



ANNEX II

Report form

Name and surname of the complainant:

Indicate your relationship with AZKOYEN (i.e. supplier, shareholder, customer, employee). If the complainant is an Azkoyen Group employee, please indicate the Department/Area to which the complainant belongs:

Address or means for notification chosen by the complainant (email, post, telephone):

Name and surname of the person reported:

Type of infringement. Please provide details on the event being report:



- Offences relating to corruption in public office
- Offences relating to corruption in business
- Offences relating to fraud
- Bankruptcy fraud / Thwarting implementation
- Offences relating to computer damages
- Offences relating to intellectual and industrial property.
- Offences relating to company secrets
- Offences against personal and family privacy
- Public finance fraud
- Crimes relating to non-compliance with or falsification of accounting obligations
- Social Security fraud
- Subsidy fraud
- Fraud against the EU budget
- Offences relating to natural resources or the environment
- Misleading advertising
- Money laundering or terrorist financing
- Smuggling
- Offences relating to risks caused by explosives and other substances
- Financial market offences
- Offences against the rights of foreign citizens
- Offences relating to public health
- Price fixing
- Fraudulent billing
- Counterfeiting of legal tender or securities
- Alteration of prices in public tenders and auctions.
- Offences against workers' rights Refusing inspection

If you wish to include additional information in this report, please indicate so in the form and we will contact you to decide how best to proceed.



- I declare that this report is made in good faith and that, excepting error or involuntary omission, the information provided is accurate. I also declare that I am aware of how the information in this report may be handled and of the content of the "Policy on Use of the Whistleblower Channel."
- The interested party expressly accepts [the Legal Notice and the Privacy Policy](#)
- The interested party expressly accepts [the information clause for the report form](#)