

WHISTLEBLOWING POLICY

Contents

1. Purpose	3
2. Definitions.....	3
3. The Whistleblowing System.....	4
4. Forms of the report.....	5
5. Investigation of the report.....	5
6. Provisions on Data Processing related to the Report	7
7. Protection of the Reporting Persons.....	8
8. Other provisions	10
9. Document history	10
Annex 1.....	11
Annex 2.....	17

1. Purpose

Taking into account Hungary's obligations under international and EU law (Whistleblowing Directive 2019/1937/EU) in line with Hungary's anti-corruption efforts and ensuring the necessary measures to protect whistleblowers as fully as possible, the Parliament, recognizing the importance of whistleblowing in the private sector as well, adopted the Act on Complaints, Whistleblowing and Whistleblowing Rules 2023. XXV of 2023 (hereinafter referred to as the "**Complaints Act**") thereby obliging **Asura Technologies Zrt.** (hereinafter referred to as „**Company**”) to create an internal whistleblowing policy (hereinafter referred to as **Whistleblowing Policy**).

It has always been of paramount importance for the Company, as an employer, to receive first-hand information from its colleagues and partners about problems, abuses, violations of interests and rights that may arise at the Company, given that complaints and whistleblowing can be good indicators for the improvement and development of processes within the Company, as well as for the elimination and prevention of situations that allow abuses. By setting up a whistleblowing system and whistleblower protection measures, our internal and external employees can receive quick and effective protection and have their complaints properly investigated, so that they can be effectively handled and contribute to maintaining a balanced, partnership-based, family-like workplace culture.

2. Definitions

1. **Report:** An oral or written notification made by the Reporting Person within the framework of this Whistleblowing System containing information concerning an unlawful or allegedly unlawful act or omission, or any other misconduct.
2. **Reporting Person:** The person who makes the Report in the Whistleblowing System.
3. **Person Concerned:** It might be a natural person or a legal entity.
4. **Other legal relationship for the purposes of work:** Every legal relationship in which the employed person performs an activity for and under the direction of the Employer for remuneration or for self-employment.
5. **Company:** who employs a natural person under a legal relationship for the purposes of work.
6. **Engaged person:** The natural person who performs an activity for and under the direction of the Company for remuneration or for self-employment based on a legal relationship for the purpose of work.

3. The Whistleblowing System

Information about illegal or suspected illegal acts or omissions or other misuse may be reported through the Company's Whistleblowing System.

The Whistleblowing System is operated by **Dr. Gábor Havas-Sághy**, a whistleblower protection attorney, on behalf of the Company in accordance with Section 50 of the Complaints Act.

Address and contact details of the whistleblower protection attorney:

- Address: 1136 Budapest, 37 Balzac Street, mf. 2.
- Phone number: (+36)1 786 66 07, Mobile: (+36)70 381 2222
- E-mail: office@hslooffice.com

Within the framework of the Company's Whistleblowing System, a Report can be made by:

- a) the Employed person by the Company;
- b) the Employed person whose Employment relationship with the Company terminated;
- c) a person who wishes to establish an employment relationship with the Company and for whom the procedure for establishing such a relationship has commenced;
- d) a self employed, sole proprietor if she/he has a contractual relationship with the Company;
- e) any person who holds an ownership interest in the Company and a person who is a member of the employer's administrative, management or supervisory body, including a non-executive member
- f)
- g) any person who is under the supervision and direction of the contractor, subcontractor, supplier or service provider that has/had a contractual relationship with the Company or has initiated the procedure to establish a contractual relationship with the Company;
- h) any trainee or volunteer who works for the Company;
- i) any person who wishes to establish a contractual relationship mentioned in point d), e) or g) if the procedure to establish the contractual relationship has commenced, and

- j) the person whose legal or contractual relationship mentioned in point d), e) or g) has terminated.

4. Forms of the report

1. The Report can be made orally (by telephone, in person) or in written form (by post, email). The personal submission of a report may be made by appointment at the office of the whistleblower protection attorney on working days.
2. The whistleblower protection attorney shall record in writing the oral report received by telephone and shall provide the whistleblower with a copy of the report, with the possibility to verify, correct and sign it.
3. If the whistleblower makes his or her report in person, the whistleblower protection lawyer shall, after having provided the information required under the provisions on the protection of personal data (Annex 1)
 - record it in a durable and retrievable form, or
 - record it in writing and, subject to the possibility of verification, rectification and acceptance by signature, shall provide a copy to the whistleblower.
4. The whistleblower protection attorney shall keep a complete and accurate record of the oral report when it is transcribed.
5. In the case of an oral report, the whistleblower protection lawyer shall draw the attention of the Reporting Person to the consequences of making a report in bad faith, to the rules of procedure governing the investigation of the Report (Annex 2) and to the fact that the identity of the Reporting Person, if he or she provides the information necessary to establish it, will be treated confidentially at all stages of the investigation of the report.
6. In the case of a written Report, the whistleblower protection attorney will send an electronic confirmation of the submission of the Report to the Reporting Person by e-mail within 7 (seven) days from the receipt of the written Report. The confirmation shall include general information on the procedural and data processing rules (Annexes 1 and 2).

5. Investigation of the report

1. The whistleblower protection attorney shall investigate the allegations contained by the Report as soon as possible but no later than 30 (thirty) days from the date

- of receipt of the Report. This deadline may be extended in particularly justified cases, subject to the simultaneous notification of the whistleblower. In this case the Reporting Person shall be informed of the expected date of the investigation and the reasons for the extension of the investigation by email. The time limit for investigating the report and informing the Reporting Person shall not exceed 3 (three) months in the event of an extension.
2. During the investigation of the Report, the whistleblower protection lawyer shall maintain contact with the Reporting Person and may invite the Reporting Person to complete or clarify the Report, to specify the facts of the case, or to provide additional information.
 3. The investigation of the report may be declined if:
 - the Report was made by an unidentified Reporting Person (the Reporting Person is unidentified if the whistleblower protection attorney has not sufficient information regarding the Reporting Person's identity despite all the effort made to discover it;
 - the Report was not made by a person entitled to make the Report as defined in Chapter 3 of this Policy;
 - the Report is a repeated report made by the same Reporting Person with the same content as the previous Report, or
 - the harm to the public interest or to an overriding private interest would not be proportionate to the restriction of the rights of the person concerned resulting from the investigation of the Report.
 4. If the investigation of the Report may be de declined pursuant to point 5.3. of this Policy, the whistleblower protection lawyer shall, until the establishment of this fact, carry out the tasks related to the receipt and recording of the Report and the providing of information related to the Report.
 5. During the investigation of the Report, the relevance of the circumstances set out in the Report shall be assessed and measures shall be taken to remedy the acts or omissions or other abuses that are or are suspected to be unlawful.
 6. If the content of the Report indicates that a criminal prosecution is justifiable, a criminal denunciation must be filed.
 7. The whistleblower protection lawyer shall inform the whistleblower in writing of the investigation of the report or of the decision not to investigate the report, the reasons for the decision not to investigate, the outcome of the investigation of the report and the measures taken or planned. The written notification can be waived only if the whistleblower protection attorney informed the Reporting Person orally who has understood the given information in a way that can be verified ex post.

8. The whistleblower protection lawyer will provide clear and easily accessible information on the functioning of the Whistleblowing System, the procedures related to the Report and on the whistleblowing systems and procedures (Annex 2).

6. Provisions on Data Processing related to the Report

1. Within the framework of the Whistleblowing System the Personal Data of
 - a) the Reporting Person,
 - b) the person whose conduct or omission gave rise to the report,
 - c) any person who may have information relevant to the subject matter of the report which are essential for the investigation of the Report, may be processed solely for the purpose of investigating the report and remedying or stopping the conduct that is the subject of the report.
2. Within the framework of the Whistleblowing System, the Personal Data that does not fall under the scope of point 6.1. shall be erased without any delay.
3. The Personal Data of the Reporting Person - with the exception of the data of the Reporting Person who has provided obviously malicious or false information - may only be transferred to the public agency or authority competent to proceed with the case initiated on the basis of the Report, if this public agency or authority is entitled to process the data by law or if the Reporting Person has consented to the disclosure of his/her data.
4. If it has become apparent that the Reporting Person has provided false data or information in bad faith and
 - a) in relation to this there are indications that a criminal offence or irregularity has been committed, the personal data of the Reporting Person shall be transferred to the public body, authority or person competent to conduct the proceedings
 - b) there are reasonable grounds to believe that the Reporting Person has caused unlawful harm or other legal prejudice to another person, the personal data of the Reporting Person shall be disclosed upon request to the public body, authority or person entitled to initiate or conduct the proceedings.
5. If the Report relates to a natural person, in exercising his or her right to information and access under the provisions on the protection of personal data, the personal data of the Reporting Person shall not be disclosed to the person requesting the information.
6. Within the framework of the Whistleblowing System, personal data can be transferred to a third country or international organization only if the recipient has

undertaken to comply with the rules on the Report under the Complaints Act and accordance with the provisions on the protection of personal data.

7. The personal data of the Reporting Person who discloses his/her identity, the person concerned by the Report or the person who may have substantial information about the facts contained in the Report shall not be disclosed to any person other than the authorized persons.
8. The Person Concerned by the Report and any person who may have material information about the facts contained in the Report shall be informed in detail about the Report, his or her rights regarding the protection of his or her personal data and the rules on the processing of his or her data at the start of the investigation. In accordance with the principle of due process, it should be ensured that the Person Concerned by a Report or in possession of material information about the facts contained in a Report can express his views on the Report through his legal representative and that he can provide evidence in support of his views. Exceptionally, and in duly justified cases, the Person Concerned by the Report or the person who has material information on the Report may be informed at a later stage if immediate information would impede the investigation of the Notification.
9. If the case cannot be investigated on the merits without the identity of the Reporting Person, the whistleblower protection lawyer shall request the Reporting Person to disclose his or her identity, taking into account that he or she is obliged to keep the identity of the Reporting Person confidential. If the Reporting Person does not provide the personal data necessary for identification at the request of the whistleblower protection lawyer, the investigation of the Report may be waived pursuant to Section 22 (6) of the Complaints Act.

7. Protection of the Reporting Persons

1. Any action is prejudicial to the Reporting Persons,
 - that was taken as a result of legitimate submission of the Report
 - that was taken in connection with the legal relationship or connection defined in Chapter 3, even if it was otherwise lawful
2. An unfavorable measure is an act or omission which is prejudicial to the Reporting Person, in particular:
 - suspension, collective redundancy, termination or equivalent measures
 - transfer of tasks, change of place of work, reduction of remuneration, change of working hours;
 - refusal to provide training;
 - negative performance evaluation or job referral;
 - the application of any disadvantageous legal consequence under the law applicable to the Employment Relationship, in particular disciplinary measures, warnings, financial sanctions
 - coercion, intimidation, harassment or ostracism;

- discrimination, unfavorable or unfair treatment;
 - failure to convert a fixed-term Employment Relationship into an open-ended employment relationship, if the Employee had a legitimate expectation that his/her employment relationship would be converted into an open-ended employment contract;
 - failure to renew or early termination of a fixed-term employment contract;
 - causing damage, including harm to the person's reputation or financial loss, including loss of business opportunity and loss of income
 - a measure as a result of which it can be reasonably concluded that the Person Concerned will not be able to establish in the future an employment relationship in the sector in which he or she is currently employed;
 - requirement for medical assessment;
 - early termination or cancellation of a contract for goods or services; and
 - withdrawal of authorization.
3. During the administrative or judicial procedures in relation to the unfavorable measures mentioned in point 7.2., if the Reporting Person proves that the filing of the Report was lawful,
- the unfavorable measure must be presumed to have been taken because the Report was lawfully made, and
 - it is for the person who imposed the unfavorable measure to prove that the adverse action was taken for a legitimate reason and not because the Report was lawfully made.
4. Where a Report has been lawfully made, the Reporting Person shall not be considered to have breached any restriction on disclosure of a legally protected secret or any other legal restriction on disclosure of information and shall not be liable in respect of such a Report if the Reporting Person had reasonable grounds to believe that the Report was necessary to discover the facts relevant to the Report.
5. Where a Report has been lawfully made, the Reporting Person shall not be liable for obtaining or having access to the information contained in the Report, unless the Reporting Person has committed a criminal offence by obtaining or having access to the information. A Reporting Person shall not be held liable for lawfully making a Report if the Reporting Person had reasonable grounds to believe that the Report was necessary to reveal the facts complained of. The Reporting Person may invoke the provisions of points 7.4 and 7.5 in all official or judicial proceedings, in addition to proving that the Report was made lawfully.
6. It is lawful to file a Report if:

- the Reporting Person has made the report in the Whistleblowing Reporting System in accordance with the rules set out in these Rules or the Complaints Act;
- the Reporting Person obtained the reported information about the circumstances to which the Report relates in the context of his or her employment-related activities; and
- the Reporting Person had reasonable grounds to believe that the reported information regarding the circumstances covered by the Report was true at the time of the Report.

7. The protection applicable to the Reporting Person shall apply to a person who
- a) assists a lawful Reporting Person in making a Report,
 - b) a person associated with the lawful Reporting Person, in particular a co-worker or family member of the Reporting Person, who may be subject to adverse action under 7.2.

8. Other provisions

1. If the whistleblower protection attorney mistakenly receives a Report concerning a defect in products manufactured or distributed by the Company, he shall immediately forward it to the competent department of the Company.
2. In matters not covered in detail by the present Policy, the provisions of the Complaints Act shall be applicable.

9. Document history

Date	Change	Last version	Creator	Verifier	Approver
28.02.2025.	Creation of document	-	Dr. Dániel Jaczó	Brigitta Bertalan	On behalf of the Board: Zoltán Szabó (COO)
15.09.2026.	Revision of document	1.0	Dr. Melissa Diki Sáfrány	Dr. Dániel Jaczó	Balázs Zirklewski

Annex 1

Information to the Reporting Person on the Protection of Personal Data**Information Notice on the processing of personal data which is strictly necessary for the purposes of the internal whistleblowing system****1. Data Controller**

- **Data Controller:** Asura Technologies Zrt. (hereinafter referred to as Data Controller),
- **HQ:** H-1122 Budapest, Városmajor utca 12-14. Building 'C',
- **represented by:** Gábor Péter Bűrchner, Balázs János Zirklewski, Ákos Csaba Takács board members
- **e-mail:** privacy@asuratechnologies.com
- **website:** <https://asuratechnologies.com/>
- **data protection officer:** Dr. Dániel Jaczó (Dr. Jaczó Dániel Law Office; seat: 1136 Budapest, Balzac u. 37., mobile: +36209148336, e-mail: daniel.jaczo@jdlaw.hu).

2. Indispensable Personal Data within the internal Whistleblowing System (hereinafter referred to as Whistleblowing System)

Whitin the framework of the Whistleblowing System a Report can be filed containing information about illegal or suspected illegal acts or omissions or other misconduct. The Reporting Person, i.e. you, may submit the Report in writing or orally. The internal whistleblowing system will process the personal data of the Reporting Person and the personal data of the person whose conduct or omission gave rise to the Report and who has relevant information in relation to the Report. All other personal data not covered by the foregoing will be erased from the reporting system without delay.

Legal basis for the Data Processing: to fulfil a legal obligation. [Article 6 (1) (c) GDPR] The Data Controller is obliged to investigate and administer the Report pursuant to Act XXV of 2023 on complaints, disclosures of public interest and rules on abuse reporting.

Purpose of the Data Processing: Only to investigate the Report about an abuse and to remedy or stop the conduct that is the subject of the Report.

Duration of the Data Processing: Personal data shall be retained until the investigation of the Report has been completed and the necessary measures have been documented, and thereafter for a predetermined period in accordance with the Company's document retention and legal claims management policies. In the event of administrative or court proceedings, personal data may be processed until the proceedings have been finally concluded or until the expiry of the applicable retention period, whichever is later.

Data Subjects: The personal data of the Reporting Party may be disclosed only to the public body or authority competent to conduct the proceedings initiated on the basis of the Report, if such public body or authority is entitled to process the data by law or if the Reporting Person has consented to the disclosure of the data. The personal data of the Reporting Person shall not be disclosed without his/her consent. Where it has become apparent that the Reporting Person has communicated false data or information in bad faith, his/her personal data shall be disclosed, upon request, to the body or person entitled to initiate or conduct the relevant proceedings.

Transferring the personal data to a third country or to an international organization:

Only in the case of a legal commitment and in compliance with the provisions on the protection of personal data.

3. Rights of the Reporting Person

In relation to data processing, you have the rights detailed in sections 3.1.-3.4. If you wish to exercise any of these rights, please write to us using one of the contact details below:

- **Address:** Asura Technologies Zrt., H-1122 Budapest, Városmajor utca 12-14. Building 'C'.
- **E-mail:** privacy@asuratechnologies.com

Identification

We will always need to identify you before we can process your request. If we cannot identify you, we will unfortunately not be able to fulfil your request.

Responding to the request

After identification, we will provide you with information about your inquiry in writing, electronically or, at your request, orally. Please note that if you have submitted your request electronically, we will respond electronically. You will of course have the option to request another method in this case.

Deadline for dealing with a case

We will inform you of the action taken regarding your request within thirty (30) days of receiving it at the latest. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further 2 (two) months, and you will be informed within the 30 (thirty) daytime limit.

We are also obliged to inform you of any failure to act within the 30-day time limit. You may lodge a complaint with the National Authority for Data Protection and Freedom of Information (point 4.1) and exercise your right to a judicial remedy (point 4.2).

3.1. You may request information (access)

You may request information on whether your personal data is being processed and if so:

- What is the purpose?
- What kind of data is being processed?
- To whom are these data transferred?
- How long do we store this data?
- What rights and remedies do you have in this regard?
- Who gave us your data?
- Do we make automated decisions about you using your personal data? In such cases, you can also request information about the logic (method) we use and the relevance and likely consequences of such processing.
- If you have found that we have transferred your data to an international organization or to a third country (non-EU Member State), you can ask for a description of how we guarantee the fair processing of your personal data.
- You can request a copy of the personal data we process. (We may charge a fee based on administrative costs for additional copies.)

3.2. Right to rectification

You may ask us to rectify or complete the personal data that we have recorded about you that is inaccurate or incomplete.

3.3. Right to erasure

You can ask us to erase your personal data if:

- The personal data is no longer necessary for the purposes for which it was processed;
- Where the processing is based solely on your consent;
- If your objection is effective;
- If we are found to be processing your personal data unlawfully;
- Where required by EU or national law.

We may not delete personal data where it is necessary:

- For the exercise of the right to freedom of expression and information;
- to comply with an obligation under Union or Member State law that requires the controller to process personal data; or in the public interest;
- in the public interest in the field of public health

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, where deletion would be likely to render impossible or seriously impair such processing; or
- for the establishment, exercise or defense of legal claims.

3.4. Right to restriction of processing

You may request that we restrict processing if one of the following conditions is met:

- You contest the accuracy of the personal data, in which case the restriction will apply for the period of time that allows us to verify the accuracy of the personal data;
- The processing is unlawful, but you oppose the erasure of the data and instead request the restriction of their use;
- We no longer need the personal data for the purposes of the processing, but you require them for the establishment, exercise or defense of legal claims;
- You have objected to the processing; in this case, the restriction applies for a period of time until it is determined whether the legitimate grounds of the Controller prevail over your legitimate grounds.

In the event of restriction, personal data, except for storage, may only be processed with your consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal entity or for important public interests of the Union or of a Member State. You will be informed in advance of any lifting of the restriction.

4. Legal remedies

4.1. You can complain to the National Authority for Data Protection and Information Security

If you believe that the processing of personal data concerning you is in breach of the provisions of the GDPR, you have the right to lodge a complaint with the National Authority for Data Protection and Information Security (hereinafter: NAIH).

NAIH

- - Address for correspondence: 1363 Budapest, Pf. 9.
- - Address: 1055 Budapest, Falk Miksa utca 9-11.
- - Phone: +36 (1) 391-1400
- - Fax: +36 (1) 391-1410
- - Web: <http://naih.hu>
- - E-mail: ugyfelszolgalat@naih.hu

4.2. You can have a claim brought before the Court of Justice

If you believe that the processing of personal data concerning you is in breach of the provisions of the GDPR and that your rights under the Data Protection Regulation have been infringed, you have the right to take legal action.

The court of first instance will have jurisdiction to hear the case. The lawsuit may also be brought, at the discretion of the data subject, before the courts for the place where the data subject resides or is domiciled. A person who does not otherwise have legal capacity to sue may also be a party to the lawsuit. The Authority may intervene in the proceedings in order to ensure that the person concerned is successful.

4.3. Compensation and damage

If the Data Controller causes damage or infringes the personal rights of the data subject by unlawfully processing the data subject's data, the Data Controller may be liable to pay damages. The controller shall be exempted from liability for the damage caused and from the obligation to pay the damage fee if it proves that the damage or the infringement of the data subject's personality rights was caused by an unforeseeable cause outside the scope of the processing.

5. Data security

We will make every effort to implement appropriate technical and organizational measures to ensure a level of data security appropriate to the level of risk, taking into account the state of the scientific and technological knowledge, the cost of implementation, the nature of the processing and the risk to the rights and freedoms of natural persons.

Personal data will always be treated confidentially, with limited access, encryption and to the maximum extent possible resilience, ensuring recoverability in the event of a breach. Our systems are regularly tested to guarantee security. In determining the appropriate level of security, we take into account the risks arising from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transferred, stored or otherwise processed.

We will take all reasonable steps to ensure that persons acting under our control who have access to personal data are only allowed to process that data in accordance with our instructions, unless they are required to do otherwise by EU or Member State law.

Annex 2

Informing the Reporting Person about the procedural rules

Information on the operation of the Whistleblowing System, the procedure for making a report, and the whistleblowing systems and procedures under the Complaints Act

Dear Reporting Person!

In accordance with Act XXV of 2023 on Complaints, Public Interest Disclosures and Reporting of Abuses (hereinafter referred to as the "Complaints Act") and the provisions of the Whistleblowing System of Asura Technologies Zrt. I hereby provide you with the following information.

What is the Complaints Act about?

It provides an opportunity for Reporting Persons to report abuses, irregularities and violations of rights in the workplace and in relation to partners and suppliers, while it imposes an obligation on the complainant to investigate complaints and to keep the identity of the Reporting Person confidential, and to establish safeguard procedures to ensure that no negative actions against the Reporting Person are applied.

Who are entitled to file a Report?

- employees;
- future employees (for example: applicants);
- former employees;
- member or owner of a business;
- member of the supervisory board;
- trainees, volunteers;
- past, present and future sub-contractors, suppliers, contractors.

What can be reported?

Any unlawful or suspected unlawful act, omission or other misconduct, information or suspicion, such as discrimination, abuse of power, attempted bribery, racism, sexism, violations of privacy, breach of contract, etc.

How to make a Report?

In writing to the whistleblower protection lawyer appointed by Company:

- By post
- By e-mail

Orally to the whistleblower protection lawyer appointed by the Company:

- By telephone
- In person (by appointment)

Asura Technologies Zrt. operates its own internal whistleblowing system with the assistance of a whistleblower protection lawyer on behalf of the Company in accordance with Section 50 of the Complaints Act.

Information on internal whistleblowing systems and procedures under the Complaints Act

What is the Employer's (complainant's) obligation following the Report?

It is obliged to provide the Reporting Person with feedback on the commencement of the investigation within 7 days and to provide the information contained in the Report as soon as possible, but not later than 30 (thirty) days from the date of receipt of the Report. During the investigation of the Report, the whistleblower protection lawyer shall keep in contact with the Reporting Person, and may invite the Reporting Person to supplement or clarify the Report, to clarify the facts and to provide additional information. The investigation period may be extended to a maximum of 3 months in justified cases.

If the report justifies the initiation of criminal proceedings, the Company is obliged to arrange for a report to be filed, otherwise the Company is obliged to remedy the infringements or take action against their reoccurrence on the basis of the Reports.

The whistleblower protection lawyer is not required to investigate the Report on the grounds set out in the Complaints Act and this Policy. Such grounds include if the Report was made by an unidentified Reporting Person, if it was made by a person who is not entitled to make a Report in relation to Asura Technologies, if the same person makes the same Report as the one made previously.

The investigation of a Report shall include an assessment of the relevance of the circumstances set out in the Report and the taking of appropriate measures to remedy the acts or omissions or other abuses that are or are suspected to be unlawful.

If the Report justifies the initiation of criminal proceedings, criminal proceedings shall be initiated.

The whistleblower protection lawyer shall inform the Reporting Person in writing of the investigation or the refusal to investigate the Report and the reasons for such refusal, the outcome of the investigation of the Report, and the action taken or planned.

The written information may be waived if the whistleblower protection lawyer has informed the Reporting Person orally and the Reporting Person has expressly taken note of the information in a manner which can be verified subsequently.

Can I make an anonymous report?

Yes, but the Company is not obliged to investigate it.

The personal data of the Reporting Person who discloses his/her identity, the Person Concerned by the Report or the person who may have substantial information about the facts contained in the Report, must not be disclosed to anyone other than the authorized person. Pending the conclusion of the investigation or the initiation of formal charges as a result of the investigation, the persons investigating the Report may share information about the content of the Report and the Person Concerned by the Report with other departments or employees of the Company to the extent strictly necessary for the conduct of the investigation, in addition to informing the Person Concerned by the Report.

If the case cannot be investigated on the merits without the identity of the Reporting Person, the whistleblower protection lawyer will ask the Reporting Person to disclose his or her identity, taking into account that he or she is obliged to keep the identity of the Reporting Person confidential. If the Reporting Party fails to provide the personal data necessary for identification at the request of the whistleblowing protection lawyer, the investigation of the Report may be waived pursuant to Section 22(6) of the Complaints Act.

Which authority controls the operation of the internal whistleblowing system?

The monitoring is carried out by the Employment Inspection Authority and the Data Protection Authority, who can also carry out an audit of the Company regarding labor and data law in parallel to the internal whistleblowing system.