



Policy on Use of the Whistleblowing Channel



Policy on Use of the Whistleblowing Channel

DOCUMENT: DC-019
DATE: 18/12/20
REVISION: 3

ORYZON
Carrer Sant Ferran 74
08940 Cornellà de Llobregat
Tel: (34) 93 5151313 Fax: (34) 93 377 40 28
Web: www.oryzon.com



Policy on Use of the Whistleblowing Channel

DATE OF REVISIONS

REVISION NO.	DATE	DONE BY	DESCRIPTION OF THE CHANGE
01	29 July 2016	ORYZON	Creation of document
02	14 December 2018	ORYZON (Board of Directors)	Adaptation of points 1 and 7 to the General Data Protection Regulation Point 4: Update links to sites where the information is available
03	18 December 2020	ORYZON (Board of Directors)	Point 1: Availability of the policy. Point 2: Widening of covered persons Point 3: Widening of activities targeted Point 5.1 Prohibition of retaliation, indemnity guarantee and presumption of innocence Point 5.2: Confidentiality Point 5.3 (new): Right to be heard Point 6.1 Receipt of reports Point 7.1 Informational clause on protection of personal data Annex I. Inclusion of Criminal Misappropriation Annex II. Changes in the form



Policy on Use of the Whistleblowing Channel

Contents

1. Introduction to the Whistleblowing Channel	4
2. Persons Covered by the Whistleblowing Channel.	
Who must use the Whistleblowing Channel?	5
3. Activities targeted by the Whistleblowing Channel.	
What breaches must be reported?	5
4. Means for receiving reports. How to report breaches?	6
5. Protection of the Whistleblower.	
Can filing a report bring about unfavourable consequences?	7
6. Procedure for processing Reports	8
7. Protection of Personal Data	10
Annex I	12
Annex II	16



Policy on Use of the Whistleblowing Channel

1. Introduction to the Whistleblowing Channel

ORYZON's leadership and reputation is the result of many years of hard work. Nevertheless, inappropriate behaviour by one single employee has the potential to tarnish our image and reputation in an instant. ORYZON must therefore actively strive to prevent and avoid that possibility.

This requires that all employees, along with business partners who may act in our name and/or for our account, must pursue their activity in compliance with the applicable laws and regulations, codes of conduct and the internal policies of ORYZON.

Also, of pivotal importance is that all employees cooperate in detecting misconduct or breaches that may jeopardise ORYZON.

In this regard, the 2010 reform of the Spanish Criminal Code (Código Penal) and, most especially, the amendment enacted by Organic Law 1/2015 of 30 March 2015, heighten the need for businesses to implement models for preventing criminal risks; that is, control systems that can prevent, detect and react to any risk of criminal wrongdoing inside a company by any member of its organisation. One fundamental component of those prevention models therefore is the existence of appropriate schemes for reporting possible risks and breaches to the body responsible for overseeing the prevention model.

Also, Circular 1/2016 of 22 January 2016 issued by the Spanish State Attorney General's Office provides that said schemes for detecting breaches are an essential element for the model's validity. Heightened value is thus ascribed to the misconduct being uncovered by the company itself, as such internal detection demonstrates not only that the model is effective but also that it is part of a culture of corporate compliance.

Pursuant to the above, the implementation of the Whistleblowing Channel in ORYZON seeks to provide an effective schemes for strengthening our commitment to a corporate culture of ethics and compliance, drawing on the cooperation of all employees and partners in the detection of possible misconduct that could place ORYZON at risk.

ORYZON is setting up its Whistleblowing Channel guided by its commitment to the applicable laws and regulations, including: 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; Spanish Organic Law 3/2018 of 5 December 2018 on the protection of personal data and guarantees of digital rights; Legal Report 0128/2007 of the Spanish Data Protection Agency titled "*Creation of Internal Reporting Systems in Companies (Whistleblowing)*", and "*Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*" of the Article 29 Data Protection Working Party of the European Commission.

Lastly, there have been taken into account the requirements laid down in the aforementioned Organic Law 1/2015 regarding the characteristics that must be built into the Whistleblowing



Policy on Use of the Whistleblowing Channel

Channel in order to be able to apply the exemption from possible criminal liability of legal persons (Article 31 bis).

This Policy is available to all employees on the ORYZON Intranet, and on the corporate website (www.oryzon.com) for all of the Company's stakeholders.

2. Persons Covered by the Whistleblowing Channel. Who must use the Whistleblowing Channel?

The Whistleblowing Channel is intended for all those employees and other persons associated with the Company, such as directors, shareholders, suppliers, contractors or subcontractors and customers of Oryzon Genomics, S.A. (hereinafter, “**ORYZON**”, or “the **Company**”) who have or may have knowledge of misconduct of potential importance, including financial and accounting irregularities or a breach of law or of the rules of conduct of the Code of Ethics and Conduct with respect to the Company or committed by any other employees, director, suppliers, collaborator or, in general, any person subject to ORYZON's control and authority and acting for its account and benefit.

2.1. Who must file reports through the Whistleblowing Channel?

All employees and other persons associated with the Company, such as directors, shareholders, suppliers, contractors or subcontractors and customers of ORYZON (hereinafter, collectively and indistinctly and solely for the purposes of this document, the “Reporting Persons” or “Whistleblowers”) must report, through the Whistleblowing Channel, any breaches known to them that fall within the scope of the targeted activities, without fear of dismissal (in the case of employees) or any other type of retaliation, discrimination or penalty.

2.2. Who may be reported through the Whistleblowing Channel?

Reports may be filed on any of the persons under the authority and control of ORYZON under an employment or commercial relationship and act for its account and benefit who have committed any of the misconducts or breaches referred to in the activities described below; for example, employees, collaborators, suppliers, as well as directors and executives.

3. Activities targeted by the Whistleblowing Channel. What breaches must be reported?

The scope of application of the Whistleblowing Channel takes in the conducts defined in the Criminal Code and the crimes covered by other special laws, as detailed in **Annex I**.

In addition, also reportable through the Whistleblowing Channel are all those breaches of potential significance, including financial and accounting irregularities and conducts that are unlawful or contrary to the rules of conduct set out in the ORYZON Code of Ethics and Conduct.



Policy on Use of the Whistleblowing Channel

Not included within the scope of application of the Ethics Channel are matters involving purely labour and human resources management questions in the Company. Such issues should be dealt with through the Company's ordinary channels.

4. Means for receiving reports. How to report breaches?

There are two ways of submitting a report, at the choice, in all cases, of the reporting person:

- One is by filling out the report form that can be found in the Investors section of the corporate website (<https://www.oryzon.com/es/inversores/gobierno-corporativo/responsabilidad-social-corporativa>) and emailing it to canaldedenuncias@oryzon.com.
- The other is by completing online the electronic report form that can be found in the Investors section of the corporate website (<https://www.oryzon.com/es/inversores/gobierno-corporativo/responsabilidad-social-corporativa>).

The report form, which is attached as **Annex II** to this Policy, is at your disposal on our Intranet [N:\01 Documentos Calidad\Compliance](#) and on the ORYZON website indicated above.

Reports not made using the form might not be accepted or acknowledged, and may be rejected and destroyed without the need for any further procedure or notice.

In all events, the utmost confidentiality of the reporting person's identity will be guaranteed.

Reports submitted anonymously in good faith that include all the required information will also be accepted for consideration.



Policy on Use of the Whistleblowing Channel

5. Protection of the Whistleblower. Can filing a report bring about unfavourable consequences?

5.1. Prohibition of retaliation, indemnity guarantee and presumption of innocence

Whistleblowers who have reasonable grounds to believe the information on reported breaches is true at the time of the report and who in good faith report a conduct included within the scope of application of the Whistleblowing Channel, and those who collaborate in the investigation or help resolve it, will be protected from any kind of retaliation, threat of retaliation, attempted retaliation, discrimination or penalty by reason of the reports made. Should the Board Committee on Compliance confirm that an interested party who acted in good faith has been the object of retaliation, it will open an investigation and, as appropriate, apply the pertinent disciplinary measures to the persons responsible for the retaliation.

The prohibition of retaliation referred to in the preceding paragraph will not impede the adoption of such appropriate disciplinary measures as may be appropriate if the internal investigation establishes that the reporting person knowingly submitted a false report. In accordance with articles 456 et seq. of the Spanish Criminal Code, false accusations or reports and the fabrication of criminal accusations are considered criminal misconduct and punishable by imprisonment of up to two years.

ORYZON shall guarantee adequate protection of the privacy and personal data and preservation of the good name, presumption of innocence and right of defence of the accused persons, especially in the event of unfounded, false or bad-faith reports, against which the appropriate disciplinary measures will be adopted.

5.2. Confidentiality

ORYZON shall guarantee the utmost confidentiality of the reports received through the Whistleblowing Channel, and of the identity of the reporting person, which shall not be disclosed without his or her express consent to any person who is not an authorised member of the personnel responsible for receiving or following up on reports. In order to ensure said confidentiality, it is expressly placed on record that exercise of the right of access by the accused person shall in no event imply access to information on the identity of the whistleblower.

All persons who learn of the reports made through the Whistleblowing Channel are obliged to maintain professional secrecy as to the identity of the reporting person.

That confidentiality obligation shall not apply when the Board Committee on Compliance or the Audit and Compliance Committee are required to disclose and/or provide information and/or documentation on their activities, including the identity of the parties involved, at the request of a competent court or administrative authority.



Policy on Use of the Whistleblowing Channel

5.3. Right to be heard

During the course of the investigation of the report, ORYZON shall guarantee the right to be heard of the Whistleblower and of the Accused, who, if applicable, may exercise their right of defence and submit the arguments, pleadings and evidence they deem appropriate.

6. Procedure for Processing Reports

6.1 Receipt of reports

All reports submitted through the Whistleblowing Channel will be received by the ORYZON Board Committee on Compliance, which shall be responsible for conducting a preliminary examination of the facts reported and deciding on whether or not an investigation should be initiated, making record of that decision.

If the facts reported do not constitute a breach falling within the scope of the Whistleblowing Channel, the report shall not be admitted for consideration and the data contained in the report will be eliminated immediately.

Where, on the other hand, the report fulfils the requisite conditions and, moreover, the facts reported fall within the scope of application of the Whistleblowing Channel, the ORYZON Board Committee on Compliance will resolve to admit it for consideration.

Any person who has been the subject of a report shall be immediately notified of **(i)** the receipt of the report, **(ii)** the accusation made against him or her, **(iii)** the departments and other persons who may receive the report and **(iv)** how to exercise his or her rights of access¹, rectification, limitation of processing, erasure, portability and objection to the processing of his or her personal data, in accordance with the applicable data protection rules.

Notwithstanding the above, if the Board Committee on Compliance concludes there is a risk that giving notice of the report could compromise the investigation, notice will be deferred until said risk disappears. In any event, the time limit for informing the accused shall not exceed one (1) month reckoned from the receipt of the report, with the possibility of that term being extended a maximum of three (3) months if there are justified reasons for doing so. All without prejudice to the law providing, expressly and obligatorily, different time limits, in which case, the latter shall prevail.

¹ The accused's right of access shall be confined to his or her own personal data processed in the report. Given the confidential nature of reports, in no event will the accused have access to the reporting person's identity and personal data.



Policy on Use of the Whistleblowing Channel

6.2 Investigation of the reported facts

After the report is admitted for consideration, the Board Committee on Compliance will commence the pertinent inquiries to establish if the reported accusations are true. For this purpose, the Board Committee on Compliance will authorise one of its members to conduct the inquiries deemed necessary to establish the veracity and reality of the reported conducts.

6.3 Proposed resolution

Once the investigation has concluded, the Board Committee on Compliance will decide, depending on the results obtained, either (i) to table the report or (ii) to formulate a proposal for a possible sanction to be levied.

In this respect, the Board Committee on Compliance will resolve to table the report and the inquiries made where sufficient evidence is not obtained for the facts reported, or where those facts do not fall within the breaches targeted by the Whistleblowing Channel.

Conversely, if the facts alleged in the report have been sufficiently evidenced and they also constitute a breach falling within the scope of application of the Whistleblowing Channel, the Board Committee on Compliance will formulate a written proposed resolution, duly reasoned, for the possible disciplinary measures to be applied.

6.4 Decision on measures to implement

To ensure the objectivity and independence of the decision, the authority and power to make the decision will rest with the ORYZON Audit and Compliance Committee in those events where the breach is considered serious.

In those cases where the breach is considered minor, the decision on the measures to be taken will rest with the Board Committee on Compliance itself.

6.5 Enforcement of the sanction

The application of the sanction or disciplinary measures that have been agreed will in each case rest with the person or persons appointed to perform said functions under a sufficient authorisation.



7. Protection of Personal Data

7.1 Informational clause on protection of personal data

In compliance with the legal requirements laid down in Spanish Organic Law 1/2015 of 30 March 2015 and 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, in Spanish Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights and in the rest of the applicable laws and regulations, the personal data obtained in the Whistleblowing Channel shall be used solely for the purpose of processing the report, investigating the veracity of the facts alleged, implementing, where applicable, such contractual, disciplinary or judicial measures as may be deemed appropriate or for pursuing such court proceedings as may apply, and said data shall be saved for so long as they remain relevant to the purpose for which they were obtained.

Personal data obtained in connection with a report and that give rise to the opening of an investigation will be included in the “Whistleblowing Channel” data processing. The data controller is Oryzon Genomics, S.A., holding Spanish corporate taxpayer identification number (CIF) A-62291919 and having its registered office at Calle Carrera de San Jerónimo 15, 2ª planta, 28014 Madrid (Spain). The information on the Data Protection Officer is as follows: Oryzon Genomics, S.A., with address at Sant Ferran 74, 08940 de Cornellá de Llobregat (Barcelona) and telephone (34) 93 515 1313.

Conversely, it is expressly placed on record that data contained in reports that are not admitted for consideration or in reports which an investigation of the facts concludes are not accurate or true will not be entered in any filing system and will be erased unless they are saved as evidence of the functioning of the model for preventing criminal wrongdoing by the company. In the latter event, the reports that have not been pursued may only be saved in anonymised form.

The data of the reporting person and of employees and other persons shall be saved in the reporting system only for the indispensable length of time required to decide on whether investigation of the facts reported is warranted.

In any event, once three months have passed after the entry of the data, they shall be erased from the reporting system. If they need to be maintained in order to continue the investigation, they may continue to be processed in a different environment by the Board Committee on Compliance.

Data obtained in an investigation of a report may be disclosed to the Board Committee on Compliance, to the Audit and Compliance Committee or, if applicable, to the Board of Directors of Oryzon Genomics, S.A., as well as to the person or persons charged with enforcing the eventual sanction. Both the whistleblower and the accused shall be duly informed, in each case, of the specific persons and bodies to which their data are to be disclosed.



Policy on Use of the Whistleblowing Channel

Lastly, the data subjects may exercise their rights of access, rectification, limitation of processing, portability and objection by emailing their request to such effect, along with a copy of their identity document, to canaldenuncias@oryzon.com. In addition, the data subjects have the right to file the relevant complaint with the Spanish Data Protection Agency (AEPD) if they believe their rights have been infringed.

Notwithstanding the above, the right of access to the report shall be limited to their own personal data, with no access to data on the identity of the whistleblower, given the confidential nature of the Whistleblowing Channel.

7.2 Principle of proportionality

Personal data obtained in the Whistleblowing Channel:

- ✓ will be limited to the information strictly and objectively necessary to be able to process the report and, as the case may have it, verify that the reported facts are true;
- ✓ will at all times be handled in accordance with the applicable data protection rules, for legitimate and specific purposes in relation to such investigation as may arise from the report;
- ✓ will not be used for incompatible purposes;
- ✓ will be appropriate and not excessive in relation to the stated purposes.

7.3 Security and confidentiality measures

ORYZON shall ensure that all necessary technical and organisational measures be adopted to preserve the security of the data obtained in order to protect them from unauthorised access or disclosures.

For these purposes, ORYZON has adopted appropriate measures to ensure the confidentiality of all the data and will make sure that data on the whistleblower's identity not be disclosed to the accused during the report, respecting in all cases the fundamental individual rights, without prejudice to such actions as may be pursued by the competent courts.



Policy on Use of the Whistleblowing Channel

Annex I

Conducts that can be reported through the Whistleblowing Channel

- ✓ **Bribery:** The offering, giving, receiving or soliciting of something of value, in whatever form, for the purpose of influencing the action or obtaining some kind of benefit for ORYZON, whether such be licit or illicit.
- ✓ **Exercise of undue influence:** Bringing undue influence to bear by taking advantage of a personal relationship in order to achieve a resolution that may generate, whether directly or indirectly, some kind of economic benefit for ORYZON.
- ✓ **Corruption in business practices:** Should an ORYZON director, manager employee or collaborator, either personally or via another person, receive, request or accept an unjustified benefit or advantage, of whatsoever kind, either for him/herself or on behalf of a third party, in consideration for unduly favouring another in the acquisition or sale of goods, or in the contracting of services, or in commercial relations. Or, on the other hand, the promise or concession of any benefit to a third party with regard to the acquisition or sale of products in commercial relations.
- ✓ **Corruption in international transactions:** Offering or handing over any undue benefit or advantage to public officers in order to obtain favourable treatment in the pursuance of international economic activities.
- ✓ **Fraud:** To deceive, for purposes of financial gain, another into taking actions or making provisions that are detrimental to the interests either of that person or of a third party.
- ✓ **Discovery and revelation of company secrets:** For the use, dissemination, revelation or cession thereof. The taking possession, by whatsoever means, of data, documents, whether on paper or digital, computerised formats or any other objects that constitute the confidential information of another company, entity, etc., for the use, spreading, revelation or cession thereof.
- ✓ **Offences against personal and family privacy:** Taking possession of, using or modifying, without authorisation and to the detriment of a third party, the reserved personal or family data of another that is registered on files or other computerised, digital or telematic, or in any public or private register or file. Illicitly accessing any computerised system in order to take possession of any personal data contained therein.
- ✓ **Tax fraud:** Defrauding the public (state, regional, district or local) tax authorities for amounts of over EUR 120,000; by avoiding the payment of taxes, retained sums, or sums that should have been retained or paid, on account of payments in kind, the undue obtaining of tax returns or the undue enjoyment of tax benefits.
- ✓ **Social Security fraud:** Avoiding the payment of Social Security payments, the undue obtaining of returns or the undue enjoyment of deductions.



Policy on Use of the Whistleblowing Channel

- ✓ **Accounting non-compliance and falsity:** Serious non-compliance with the obligation to keep a true record of the company accounts, books and/or accounting records. This type of offense usually goes hand in hand with other fraudulent conducts, insofar as it often takes the form of double-accounting and false accounting entries.
- ✓ **Subsidy fraud:** Obtaining subsidies or grants from the public administrations, for an amount, or for a value, of over twenty thousand Euros by falsifying the conditions required for the concession thereof, or by concealing those conditions that would have prevented it.
- ✓ **EU General Budget fraud:** Defrauding the budgets of the European Union, along with others administered thereby, for amounts of over EUR 50,000. Avoiding the payment of amounts that should be paid, dedicating the funds obtained to uses other than those for which they were intended, or unduly obtaining funds by falsifying the conditions required for the concession thereof or by concealing those conditions that would have prevented it.
- ✓ **Frustration of execution:** Undertaking any action with regard to the disposal of assets or the generation of obligations that obstructs or prevents the application of an embargo or a claim for payment. Concealing assets during judicial or administrative proceedings. The unauthorised use of goods that have been seized by the authorities.
- ✓ **Criminal bankruptcy:** Should it be the case that the company is in bankruptcy proceedings, this violation occurs when an attempt is made to dispose of assets in order to unduly reduce the equity that serves as a guarantee for compliance with obligations, or makes it difficult or impossible for creditors to discover the true economic situation of the debtor.
- ✓ **Infringement of intellectual property:** Reproducing, plagiarising or publicly making known, whether fully or partially, a literary (book), artistic (picture or photo) or scientific (specific theory, applications or software programs) work, or the transformation, interpretation or artistic execution thereof, in whatsoever medium or means of communication, without the authorisation of the owners thereof. For example, this violation is applicable in those cases in which software programs are used without the concession of the corresponding licence.
- ✓ **Infringement of copyright:** The reproduction, imitation, etc. of any distinctive sign without the consent of the owner thereof, in such a way that another sign is obtained that is identical to, or may be easily confused therewith, for the distinguishing of the same or similar products, services, activities or establishments.



Policy on Use of the Whistleblowing Channel

- ✓ **Digital sabotage:** Deleting, damaging, deteriorating, erasing or rendering inaccessible external data, software programs or digital documents, without authorisation and when the result thereof is serious. Preventing or hindering the operation of external computing systems.
- ✓ **Undue handling of toxic, corrosive and other substances:** Contravention of the safety regulations established for the manufacture, handling, transport, storage or sale of explosives, inflammable or corrosive substances, toxic or asphyxiating substances, specifically endangering people's lives, physical integrity or health and t/or the environment.
- ✓ **Offences involving natural resource and the environment:** Provoking or directly or indirectly being responsible for emissions, spillages, radiations, extractions, excavations or silting up; noises, vibrations, injections or deposits into the atmosphere, soil, subsoil, inland, underground or maritime waters; establishing deposits or dumps for waste or scrap materials, whether solid or liquid, toxic or dangerous that might be seriously detrimental to the balance of natural systems or people's health.
- ✓ **Offences against public health:** Offering products on the market that are noxious for health and/or that do not comply with the requirements in terms of shelf life or composition established by the applicable laws and regulations. Also, the elaboration of substances that are noxious for health, as well as the dispatch, supply or sale thereof.
- ✓ **Securities fraud:** Using or supplying information that is relevant with regard to the quotation of any kind of financial instrument. Spreading news or rumours regarding persons or companies in the knowledge that such is false and for the purpose of altering or maintaining the price or quotation of stocks, shares or other financial instruments. The falsification of economic-financial information contained in the issue prospectuses of whatsoever financial instruments or information that the entity is required to publish or publicise, pursuant to stock market legislation.
- ✓ **Illegal financing of political parties:** The illegal handing over of donations or contributions to a political party, federation, coalition or electoral group.
- ✓ **Violation of the rights of overseas citizens:** Promoting, favouring or facilitating the illegal trafficking of clandestine immigration.
- ✓ **Smuggling:** Importing or exporting licit commercial goods in an irregular way, always insofar as the value of the said property, merchandise, goods or effects is equal to or greater than EUR 150,000.
- ✓ **Money laundering:** Accepting funds, deposits, etc. that have their origin in the commission of a crime or taking part in any action to conceal such an illicit origin, or helping persons that have participated in crime. This offence may be committed imprudently, as a result of acting without due diligence, i.e. it is not necessary that the authors be aware of the crime that they are committing.



Policy on Use of the Whistleblowing Channel

- ✓ **Financing terrorism:** Providing, collecting or accepting funds with the intention that they be used, or in the knowledge that they are going to be used, to commit crimes related to terrorist organisations or groups, or to deliver them thereto. This offence may be committed imprudently, as a result of acting without due diligence, i.e. it is not necessary that the authors be aware of the crime that they are committing.
- ✓ **Trafficking of organs:** Promoting, favouring, facilitating or publicising the illegal securing of human organs, or the transplanting thereof, whether such be major organs or otherwise.
- ✓ **Misleading advertising:** Drawing up offers or advertising for products and services in which false allegations are made asserting the existence of characteristics that are false with regard thereto, in such a way that this can cause serious and manifest detriment to consumers.
- ✓ **Genetic manipulation:** Manipulating human genes to alter the genotype for any purpose other than the elimination or treatment of serious illnesses or defects. The use of genetic engineering to produce biological weapons or weapons that could exterminate the human species. The fertilisation of human ovules for any purpose other than that of human procreation, along with the practice of assisted reproduction on a woman without her consent.
- ✓ **Obstructing inspection activities:** Rejecting or preventing the actions of persons, bodies or entities that are acting as inspectors or supervisors, while being the de facto or de jure administrator of a company, either constituted or in the process thereof, and subject to or acting on markets where administrative supervision is required.
- ✓ **Infringement of worker's rights:** Placing the lives, the health or the safety of workers in serious danger through the violation of workplace risk prevention regulations. This offence may also be committed imprudently. The use of deception or abuse in a situation of need to impose employment or Social Security conditions on workers that are detrimental to, suppress or restrict, their rights. Imposing working conditions that are unsuitable or in conflict with health and safety at work; treating workers in conditions of inequality and discrimination, preventing or limiting their union rights.
- ✓ **Embezzlement of public funds:** consists of criminal misappropriation of government funds by persons responsible for the control and custody of those funds or where those persons allocate public funds to other than their intended purposes.



Policy on Use of the Whistleblowing Channel

Annex II

Whistleblower reporting form

Full name of the whistleblower:

Department / Area in which the whistleblower works:

Address or means of reporting chosen by the whistleblower (email, ordinary post, phone):

Full name and address of the party object of the report:

Type of violation/infringement (mark with an X):

- Bribery
- Exercise of undue influence
- Corruption in business practices
- Corruption in international transactions
- Fraud
- Discovery and revelation of company secrets
- Offences against personal and family privacy
- Tax fraud
- Social Security fraud
- Accounting non-compliance and falsity
- Subsidy fraud
- European Union General Budget fraud
- Frustration or execution
- Criminal bankruptcy
- Infringement of intellectual property
- Infringement of copyright
- Digital sabotage
- Undue handling of toxic, corrosive and other substances
- Offences involving natural resources or the environment
- Offences against public health
- Securities fraud
- Illegal financing of political parties
- Violations of the rights of overseas citizens
- Smuggling
- Money laundering



Policy on Use of the Whistleblowing Channel

-
- Financing terrorism.
 - Trafficking of organs
 - Misleading advertising
 - Genetic manipulation
 - Obstructing inspection activities
 - Infringement of workers' rights
 - Embezzlement of public funds
 - Failure to comply with laws, policies, regulations and internal procedures
 - Other

Attach the documentary support on which the report is based, should such exist.

I hereby state that the present report has been made in good faith and that, excepting inadvertent errors or omissions, the data attached hereto are true.

Likewise, I also hereby state that I know the treatment that could be dispensed to the data attached in the present report, along with the contents of the "Whistleblowing Channel Use Policy".

This present document will be held at the offices of Oryzon Genomics, S.A., pursuant to their Document Filing and Conservation Policy, with a copy hereof being handed over to the Whistleblower.