CRG INTERNAL INFORMATION CHANNEL REGULATION

Index

1. Introduction and Purpose of the Regulation

The CRG has implemented its Internal Information System and its Internal Information Channel as a preferential channel available to all employees, researchers, technicians, students, third party collaborators, suppliers, as well as any other third party, to communicate possible breaches or violations of the provisions of any of the organisation's internal policies, as well as any infringement or omission of which they are aware and which may involve a breach of European Union law or its financial interests or criminal or administrative offences within the Spanish legal framework, as explained in the CRG's Internal Information System Policy.

For this purpose, the Internal Information Channel can be accessed through the address compliance@crg.eu, with the possibility of sending communications or reports by post to the Fundació Centre de Regulació Genòmica, Carrer Doctor Aiguader, number 88, Edifici Parc de Recerca Biomédica de Barcelona (PRBB), 08003, for the attention of the Compliance Committee, who has been designated as the person responsible for this System. Additionally, informants may communicate alerts verbally to the Coordinator of the Compliance Committee, by telephone to his/her direct number, or by means of a face-to-face meeting, directing the request through any of the aforementioned means of communication, with the possibility of sending communications or reports anonymously.

This Regulation develops the procedure for communications management procedure, which establishes the necessary provisions for the Internal Information System complies with the requirements established in Spanish Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (hereinafter, 'Law 2/2023, of 20 February').

Although the Internal Information System is the preferred means, alternatively, any natural person may report to the Independent Authority for the Protection of Informants (hereinafter, 'A.A.I.') or to the corresponding regional authorities or bodies, the commission of any action or omission, either directly or after prior communication through the aforementioned Internal Information Channel and in accordance with the terms established in the aforementioned Law 2/2023, of 20 February.

2. Stages of the communications management procedure

2.1. Receipt of communications stage

At the CRG, the reception of all communications made through the Internal Information System shall be managed by the Head of the Internal Information System, who shall at all times guarantee respect for the independence, confidentiality, data protection and secrecy of communications. As this is a collegiate body, the Head of the System delegates to the Coordinator of the

Compliance Committee, who acts as Delegated Manager, the powers to manage the Internal Information System and to process investigation files.

Said communication shall be made **in writing**, either anonymously or by name, being in any case confidential and including a description of the facts, the identification of the persons involved and, if possible, providing evidence accrediting the breach reported and explaining the circumstances in which access to said information has been obtained.

The communication may also be made **verbally**, either in person or by telephone. The informant may request a face-to-face meeting with the Delegated Manager of the Internal Information System, which shall be held within a maximum period of 7 (seven) days from the request, in the manner deemed most convenient by the organisation and preserving the confidentiality of the information. The information received through this meeting shall be recorded and the communicator shall be warned of this circumstance. The communicator will also be warned about the processing of his/her personal data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, in Organic Law 3/2018 of 5 December on the Protection of Personal Data and guarantee of digital rights, Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties, and the aforementioned Law 2/2023 of 20 February. Alternatively, the meeting may be documented by means of a complete and accurate transcript of the conversation. Following this referral, its processing and management shall be carried out in accordance with this Regulation.

If the communication is received through internal channels other than those established by the CRG or is addressed to members of staff not responsible for its processing, the organisation shall likewise guarantee the preservation of confidentiality, warning whereas failure to comply would imply a very serious breach of the Law and that the communication would be immediately forwarded to the Head of the System.

Once a communication or information has been received, the Head of the System is the body responsible for initiating the corresponding investigation process, where appropriate, to clarify the facts that are the object of the communication.

An **acknowledgement of receipt** shall be sent to the informant within 7 (seven) calendar days of receipt of the communication. This acknowledgement of receipt shall be included in the file including, in any case, clear and accessible information on the external information channels with the competent authorities.

In cases whereas an acknowledgement of receipt could jeopardise the confidentiality of the communication, in order to ensure confidentiality, it shall not be made until a period of time deemed prudent has elapsed.

As mentioned in previous paragraphs, as an alternative to this preferred Internal Information System, it is possible to report to the A.A.I. or to the corresponding regional authorities or bodies, of the commission of any action or omission which may constitute any of the infringements that may be reported through the Internal Information System[1], either directly or after prior notification through the aforementioned System, following the provisions of **Annex 1** on external information channels.

2.2. Communications admissibility stage

After receiving the report, the Delegated Manager will assign it a **registration number** that will correspond to its file and a series of codes to anonymise both the data of the informant and of the investigated party, the facts, and any other third party that may be affected by the report.

Firstly, the Compliance Committee (as the collegiate body responsible for the Internal Information System) will check that neither the Delegated Manager, nor any other member of the Committee itself, nor any member of their respective departmental work areas, are involved in said communication. If this is not the case, the person and/or area involved shall be required to step down and shall be replaced in order to guarantee due impartiality. This shall be recorded in writing in the file. The rule on this conflict of interest shall be:

1. If the Delegated Manager or a person from the same area of work is involved, the investigation shall be taken over by another member of the Committee.

2. If other members of the Committee or persons from their respective areas of work are implicated, the Delegated Manager shall continue the investigation.

3. If all members of the Committee are involved, the investigation shall be followed by the Substitute appointed by the Governing Body to carry out these particular cases.

These replacements and new appointments shall be recorded in writing in the minutes and in the opening of the file.

Finally, upon receipt of the communication, the Head of the System shall record the following information, among others:

- The objective data of the communication: facts that are the object of the report, names of the perpetrators or participants in the facts that are the object of the report, dates, quantities, places, contacts, and information associated with the facts reported, provided by the communicator/reporter.

[1] In this regard, see Section 3 'Content of communications', of the Internal Information System Policy.

- Subjective data: opinions, ideas and appraisals of the reporter/reporter that he/she considers necessary when describing the communication.

- Assessment by the Head of the System as to whether the report is associated with criminal conduct or whether it is a mere complaint or suggestion regarding improvement of an area of the centre, work situation, etc.

If the Head of the System notices that the facts reported could be indicatively constituting a crime, he/she shall immediately forward the information to the CRG's Director and Administrative Director and its governing body, which shall decide on its referral to the competent public authority.

2.3. Investigation stage

In the event that the report is accepted for processing, the general rule is that the investigation will be conducted by the Head of the System and carried out by him/her[2].

If possible, the reporting person may be asked to provide additional information necessary for the course of the investigation to which his or her report has given rise.

At this stage, the **person under investigation shall be notified and interviewed**, informing him/her of his/her right to be informed of the actions or omissions attributed to him/her, and he/she may also exercise his/her right to be heard, without in any case being informed of the identity of the informant.

The third **parties involved (if any) shall also be summoned and interviewed** so that they may explain and indicate the allegations they deem appropriate. Any investigative steps that may be necessary for the parties shall be carried out and a record shall be made in the file.

In the event that the matter is related to scientific malpractice, the provisions of the Procedure in cases of suspected scientific malpractice of the CRG shall apply.

Inquiries made to third parties or other bodies or areas of the CRG must be carried out in such a way as to maintain the **anonymity of the communicator/reporter and the person under investigation**, as well as the reasons for the communication.

The **confidentiality** of the information, as well as the **presumption of innocence and respect for the honour** of all persons affected shall be guaranteed at all times.

[2] Except in cases of conflict of interests.

During this stage, the Head of the System:

1st. Shall investigate the facts communicated and, specifically:

- The objective and subjective elements provided by the communicator/ informant, prioritising the objective elements supported by documentation that accredits, in whole or in part, the facts communicated.
- The reputation, seriousness and reliability of the communicator/reporter.
- The allegations and defence evidence provided by the investigated party.
- The evidence provided to third parties, or to other related bodies or areas.

2nd. Shall analyse and assess the possible consequences that the reported facts may produce:

Firstly, the Head of the System shall check whether these events occurred due to a significant lack of internal controls in the CRG. If so, he/she will propose urgent mitigating and preventive measures to avoid new risks.

If the Head of the System deems it appropriate, he/she may request assistance from Director and/or the Administrative Director for the investigation. However, if the reported event involves a member of Director and/or the Administrative Director, the Compliance Committee shall refrain from requesting the collaboration of that member.

Secondly, if the seriousness, speciality or complexity of the facts makes it advisable, the Head of the System may appoint another person in charge of the management or scientific area or a specialised third party to collaborate in the investigation. If, as a result of the reported facts, losses of assets may occur, the Head of the System shall take measures to halt or mitigate such losses or damage. If there may be a leak or destruction of evidence relevant to the investigation, prior to the commencement of the investigation, the Head of the System shall be responsible for securing evidence. The Head of the System shall also assess the appropriateness of informing the governance bodies of this communication. Finally, he/she shall check whether there is a possibility that damage has been caused to third parties, in which case, he/she shall assess the extent of the damage and the need to inform the injured third party.

The time period for carrying out the investigation and providing a response to the informant on the actions that have been carried out, as well as the result thereof, will depend on the seriousness of the facts reported and their potential consequences, the duration of this stage being at the discretion and risk of the Head of the System. However, in accordance with the provisions of article 9.2. d) of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, this period may not exceed 3 (three) months from receipt of the report or, if no acknowledgement of receipt was sent to the informant, 3 (three) months from the expiry of the period of 7 (seven) days after the report was

made[3]. This, except in cases of particular complexity, where the time limit may be extended for up to a maximum of a further 3 (three) months.

If the communication contains personal data of third parties other than the person under investigation (e.g. witnesses, suppliers, etc.), the Head of the System shall record in writing that all personal information provided that is not necessary for the investigation must be deleted, and proceed to inform the third parties whose data are to be processed. The information shall comply with the information requirements of the data protection regulations, omitting from this information the identity of the informant, which shall be kept confidential.

All these notifications shall be decided by the Head of the System and shall be recorded in writing in the file.

2.4. Finalisation procedure stage:

If the communication contains personal data of third parties other than the person under investigation (e.g. witnesses, suppliers, etc.), the Head of the System shall record in writing that all personal information provided that is not necessary for the investigation must be deleted, and proceed to inform the third parties whose data are to be processed. The information shall comply with the information requirements of the data protection regulations, omitting from this information the identity of the informant, which shall be kept confidential.

After the investigation of the communication and with the accrediting documentation that serves to clarify the facts, a **Verdict or Resolution** will be drawn up with the following content:

- Description of the facts: record no. of the communication; date of the communication; facts reported; intervening parties; documentation provided throughout the investigation by both parties (communicator/ informant and investigated), by other bodies, areas or departments of the organisation or by third parties; interview with the investigated party and/or with third parties, etc.
- Analysis and assessment of the evidence obtained.
- In the event that the reported irregularity is indeed proven, the Head of the System will dedicate a section of the verdict to make the recommendations that he/she considers necessary to implement in order to improve the internal controls and protocols that have been deficient on this occasion.
- Resolution: after approval by the CRG Director and Administrative Director, or by the CRG governing body in the event that the decision must be approved by the same, this resolution must be substantiated and contain the reasons for which the decision is to be FILED WITHOUT SANCTION or FILED WITH SANCTION.

[3] These deadlines shall be complied with, in any case, without prejudice to the provisions of the labour regulations or collective bargaining agreement applicable to each case, whose deadlines shall prevail in the event of contradiction or potential breach of regulations.

I. FILING WITHOUT SANCTION: After investigation, if it is concluded that the reported infringement is manifestly minor and does not require further follow-up, it shall be filed. The case of repeated communications that do not contain new and significant information on previously reported infringements and whose investigation procedure has already been concluded shall also be closed, unless there are new factual or legal circumstances that justify a different follow-up. In such cases, the decision must be communicated to the informant and the reasons for the decision must be given. Also, internally, actions shall be taken to ensure that the reported facts are not repeated in the future. These actions may include implementing additional controls, reviewing policies and procedures, and conducting training to improve conduct and regulatory and ethical compliance.

II. ARCHIVE WITH SANCTION: The Head of the System may propose the application of a sanction, but the decision will be made by the CRG Administrative Director in coordination with the People and Legal areas, in accordance with the procedures indicated for the application of labour sanctions in the organisation.

III. COMMUNICATION TO THE AUTHORITIES: If the communication received a priori appears to be related to the commission of a crime, the Head of the System shall immediately report it to the CRG Administrative Director in order to assess the possibility of reporting it to the competent authorities. Moreover, if the reported facts are already under investigation by judicial or police authorities, the CRG will fully cooperate and monitor the results of such investigations. This will enable any further impact to be assessed and appropriate action to be taken in line with the law.

In this sense, Article 259 of the Spanish Criminal Procedure Act provides that anyone who witnesses the perpetration of any public offence[4] is obliged to immediately report it to the examining magistrate, justice of the peace, regional or municipal judge, or public prosecutor nearest to the place where he or she is[5].

For its part, the duty to report to the competent authorities is increased with regard to certain offences distinguished by the criminal law. In this respect, Article 450 of the Spanish Criminal Code provides for the 'omission of the duty to prevent crimes or promote their prosecution', punishing anyone who fails to prevent the commission of a crime affecting people's life, integrity or health, freedom or sexual freedom, when they could have done so with their immediate

[4] The classification of an offence as a public offence is related to the person who instigates its prosecution (ex officio or by the injured party), with **public offences** being prosecutable ex officio without the need for a prior complaint by the injured party. In addition to crimes against life and liberty, in the catalogue of crimes that generate criminal liability of the legal person we find, by way of example, the following public crimes: fraud, bribery, influence peddling, money laundering, financing of terrorism, crimes against the Public Treasury and Social Security, crimes against the environment and natural resources, crimes against regional planning, against fundamental rights and public liberties, smuggling, among others). On the other hand, slander and libel between private individuals are **private offences** (the justice system can only act when the injured party files a complaint) and **semi-public offences** can be prosecuted ex officio once the injured party has initially filed a complaint (offences of discovery and disclosure of secrets, offences against intellectual property, assaults, harassment and sexual abuse, and collusion), among others.

[5] According to the current literal wording of Art. 259 of the Spanish Criminal Procedure Act.

intervention and without risk to themselves or others, and anyone who, when they could have done so, does not go to the authorities or their agents to prevent one of these crimes, of which they are aware that they are about to commit or are currently committing.

With regard to the **sanctioning regime**, if, once the investigation of the facts has been completed, their veracity is confirmed, the CRG will take all the necessary measures to put an end to the reported fact and, if appropriate and taking into account the characteristics of the fact, will apply the actions it deems appropriate as set out in the disciplinary regime and the labour legislation in force, in accordance with the aforementioned criminal legislation.

The measures that may be imposed internally shall not limit, at any time, the exercise of legal actions that may be taken by the organisation.

In all cases, both the communicator/reporter and the person under investigation **shall be notified of the Resolution**, taking into account the maximum period of 3 (three) months from the receipt of the communication. The informant shall not be notified if he/she has waived this, if no contact details are available or if the informant is anonymous.

Once a Resolution has been adopted on the communication, the Head of the System shall order the ARCHIVING and the BLOCKING OF THE RECORDS of the same, for such period as he/she deems prudent until its total elimination, respecting in any case, the legislation in force on personal data protection.

In case of ARCHIVE WITH SANCTION, the notification to the investigated person will contain the adoption of the contractual, disciplinary or judicial measures to be taken.

The CRG guarantees that no retaliation will ever be taken against any person who in good faith brings a criminal offence to the attention of the organisation, assists in its investigation or helps to resolve it. This guarantee does not extend to those who act in bad faith with the intent to spread false information or to harm individuals. The CRG shall take appropriate legal or disciplinary action against such misconduct.

3. Register of communications

The Head of System maintains a logbook of the information received and the internal investigations to which it has given rise, which is used to store and/or retrieve key information on each incident, including the date and source of the original communication, the plan of the investigation, results of interviews or any other investigative procedures, outstanding tasks, final resolution, as well as the chain of custody of any key evidence or information.

4. Personal data protection

As set out in the CRG's Internal Information System Policy, the processing of personal data arising from the application of this Policy and of this Communication Management Procedure is governed by the provisions of Title VI of Law 2/2023 of 20 February, by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, by Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights, and by Organic Law 7/2021, of 26 May, on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties.

Considering the data minimisation principle of the General Data Protection Regulation contained in Law 2/2023 of 20 February, the CRG will only process personal data necessary for the purpose of knowledge and investigation of the actions or omissions under investigation through the Internal System. Consequently, to the extent that the personal data collected is not considered necessary or if it is proven that it is not truthful information, the CRG will proceed to its deletion under the terms established in article 32 of Law 3/2018[6].

Likewise, the CRG may only process special category data[7] to the extent that such data are necessary for the adoption of the corresponding corrective measures or sanctioning procedures that may eventually have to be carried out, failing which they must be immediately deleted under the aforementioned terms.

Lastly, the CRG must guarantee that the subjects affected by the processing of personal data carried out as a result of the investigation may exercise their rights of access, rectification of inaccurate data, erasure, limitation, portability and objection, bearing in mind that the right of access may not include information on the informant and that the right of objection of the persons under investigation may be denied for legitimate reasons

[6] When deletion is appropriate, ONECHAIN shall block the data by adopting any measures necessary to prevent the blocked information from being processed (except for making it available to the judicial authorities, the Public Prosecutor's Office (Ministerio Fiscal) or the competent public administrations for the purpose of demanding possible liabilities) for the time necessary to keep evidence of the operation of the system which, considering the statute of limitations indicated in Law 2/2023, of 20 February, is set at 3 years. It should be noted that the obligation to block and retain does not apply to personal data contained in communications that are not investigated and may only be retained in anonymised form.

[7] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data relating to health, sex life or sexual orientation of a person.

5. Security and Confidentiality

The electronic communications channel will have an assigned System Administrator in the ICT department of the CRG, in charge of establishing and customising the necessary security of the system, including restricting access and the ability to lock records, which should not be able to be modified once they have been recorded. Special management and administration is foreseen for the deletion of records from the system.

In addition, the mailbox will be able to audit access to individual records and record the date, time and user name, including any modifications made to the records.

In order to ensure that the data maintained is as accurate as possible, communications that are not relevant and those which, upon investigation, are found to be inaccurate or untrue shall be deleted immediately.

Likewise, the communications mailbox will allow the Head of the System to store and/or retrieve key information on each incident, including the date and source of the original communication, the investigation plan, results of interviews or any other investigation procedure, pending tasks, final resolution, as well as the chain of custody of any evidence or key information.

Finally, it is recalled that the confidentiality of the informant and the reported party will be maintained at all times, and their identities will not be disclosed outside the sphere of the Compliance Committee and the Head of the System.

6. Regulation Monitoring and Control

The implementation, compliance, and updating of this Regulation will be supervised by the CRG Compliance Committee.

This Regulation will be reviewed and/or modified by the Compliance Committee whenever relevant changes occur in the organization, in the control structure, or the activity carried out by the organization, making it advisable that there are legal modifications, or revealing the need to update its provisions. The Committee may outsource this service to specialist professionals.

This Regulation will be reviewed at least every two years, even if none of the circumstances described above occur.

7. Related documentation

1. CRG Code of Conduct and Good Governance.
2. Anti-Fraud Measures Plan.
3. Criminal Compliance Manual.
4. CRG Criminal Compliance Policy

5. CRG Internal Information System Policy

8. Approval of this Regulation

These Internal Information Channel Regulation of the CRG has been approved as indicated in the versions track-record below and may be amended in order to maintain at all times the culture of compliance within the organisation, embodied in the principles of transparency, accountability and prudence towards third parties and towards its own members and business partners.

9. Versions track-record

Version	Date	Approved by	Reason for change
V.1	11/28/2022	CRG Coordinator of the Compliance Committee and Administrative Director	
	12/15/2022	CRG Board of Trustees	
V.2	11/29/2024	CRG Coordinator of the Compliance Committee and Administrative Director	Adaptation to Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (regarding the content of the phases of the communications management procedure, the functions of the Head of the System, the register of communications and the aspects of personal data protection).
	12/19/2024	CRG Board of Trustees	

10. Annexes

REPORTING FORM

IDENTIFICATION DATA OF THE COMPLAINANT/INFORMANT

Given name and surname of the informant	
Email address	
Postal address (optional)	
Telephone number (optional)	
CRG area or department in which they provide their services	

REPORT

Description of the report (if possible, attach evidence or supporting documents for the report)	Please identify persons (physical and/or legal) that have participated in the acts, in what capacity, the type of relationship that you have with the person being reported, and whether or not there are more people who know about the acts (indicate who)
	Please indicate the reason for the report (facts and evidence), the time frame in which this took place, the affected area(s) of CRG, and all those facts that are to be considered.

Is there any conflict of interest with any of the members of the CRG Compliance Committee?

☐ Yes Indicate with whom: Click or tap here to write text.

☐ No

External information channel-Independent Authority for the Protection of Informants, A.A.I.

All natural persons may report **to the state A.A.I. or to the corresponding regional authorities or bodies** through the external channels duly set up for this purpose, the commission of any actions or omissions referred to in the CRG's Internal Information System, either directly or by prior communication through the CRG's Internal Information Channel.