CRG COMMUNICATIONS CHANNEL REGULATION

Index

1. Introduction and Purpose of the Regulation

The CRG Foundation expects both its members and its collaborators, suppliers, and the third parties that work with CRG, to act at all times in accordance with the principle of good faith in the performance of their functions. This requires, among other aspects, maintaining an ongoing attitude of collaboration with the organization.

The purpose of this Regulation is to establish and regulate the procedure for receiving and processing communications and reports of behaviors that contravene that which is stipulated in the Anti-Fraud Measures Plan, the Code of Conduct and Good Governance, its Criminal Compliance Manual, its regulations on Personal Data Protection, as well as the rest of the CRG internal Policies and Protocols, guaranteeing confidentiality for both the complainant/informant and the person who has been reported at all times.

2. Objective and Subjective Scope of the Channel

CRG has designed and implemented a communication channel as a tool for enabling compliance with the above. In this way, the members of the organization, suppliers, and the third parties that work and collaborate with CRG, can indicate or communicate reports on irregularities that they detect in the performance of their duties, as well as any inquiries or questions that relate to the interpretation of the foundation's internal policies and rules.

This communication channel will only be used for the purpose described, and will not be used as a vehicle to present labor or organizational complaints.

As a general principle, in the event that any member or collaborator has doubts or suspicions regarding a possible violation of current legislation, the Code of Conduct and Good Governance, the Anti-Fraud Measures Plan, the Criminal Compliance Manual, or any other internal policy or protocol applied by CRG to ensure lawful, safe, and transparent activity, they should communicate this situation through the communications channel established for this purpose.

A postal mailbox and an email address are made available to everyone for this purpose, to allow people to communicate any information or evidence of an irregularity or criminal action within the scope of the foundation's activity to the Compliance Committee.

These communications shall be sent with the sender named, confidentially, and explaining the circumstances under which said information has been accessed through the Communications Channel at the address compliance@crg.eu, although it is also possible to send communications anonymously, via postal mail to Fundació Centre de Regulació Genòmica, Carrer Doctor Aiguader 88, Edifici Parc de Recerca Biomèdica de Barcelona (PRBB), 08003, for the attention of the Compliance Committee.

In the event that the communication is related to a fact or irregularity that is related to the CRG Compliance Committee, it will be sent to the immediate supervisor, so that they can proceed to manage the replacement of that member of the Compliance Committee. Another executive member, whose personal and professional characteristics are suitable for the post, will be brought in, in line with the competences described in the Criminal Compliance Manual and the Anti-Fraud Measures Plan. This replacement and new appointment will need to be stated in writing, in the minutes of the opening of the investigation file.

CRG's communications mailbox is a secure tool where all incidents that are received will remain recorded, as well as any action that is taken in relation to them.

CRG's communications mailbox is managed and operated by the Compliance Committee.

3. Requirements for acceptance and processing of communications

In order for communications or reports received via the email channel to be accepted and processed, they should contain, as a minimum:

- The identity of the complainant/informant
- A description of the facts that are the subject of the report, in a clear, detailed manner
- Evidence upon which the complainant/informant's report is based
- The identity of the person who has been reported, in the event that the complainant/informant knows the perpetrator of the acts that are the subject of the report
- The time frame within which the acts that are the subject of the report were carried out.

In the event that the complainant/informant prefers to remain anonymous, they will be able to present their communication or report in such a way that, in order for it to be accepted and processed, it will need to comply with all the aforementioned requirements except for the reference to the identity of the complainant/informant.

The communication should be accompanied by all those pieces of evidence that the complainant/informant has at their disposal.

In order to facilitate the communication of acts that are contrary to the stipulations in the Anti-Fraud Measures Plan, the Criminal Compliance Manual, the Code of Conduct and Good Governance, and other internal CRG rules, and in order to comply with the indicated minimum requirements, it is recommended to use the Communications Channel Form that is attached in Annex 1 of this Regulation.

4. Communications Procedure

Unless CRG opts to outsource the communications management system, the Compliance Committee is authorized to lead investigations that come about as a consequence of a valid communication. The communications procedure that will be followed in CRG is as follows:

1ST PHASE: ACCEPTANCE OF COMMUNICATIONS AND NOTIFICATIONS

The Compliance Committee Coordinator will have access to the postal mail and the email account of the Communications Channel.

After the communication is received, it will be transferred to the members of the Compliance Committee, who should assign it a REGISTRATION NUMBER and create a FILE, and check that their area is not involved in said communication. If this is the case, the Committee member whose area is affected will remove themselves from the investigation in order to guarantee the necessary impartiality. This situation will be stated in writing in the minutes, and in the opening of the file.

In this case, the Compliance Committee member should be replaced by a member whose personal and professional characteristics are suitable for the post, a situation which should also be stated in writing in the minutes of the opening of the file.

Likewise, in the event that a Compliance Committee member acquires knowledge, by any means, of a fact that should lead to the initiation of an investigation, they are authorized to initiate that procedure of their own accord.

Finally, within 72 of receipt of the communication, the Compliance Committee should record the following information through the minutes:

- The objective data from the communication: facts, dates, names, quantities, places, contacts, etc., that the person who sent the communication provides.
- The subjective data: opinions, rumors, ideas, etc., assessments of the complainant/informant when describing the communication.
- Assessment of the Compliance Committee on whether the communication is associated with criminal conduct, or if it is merely a claim or a suggestion relating to improving an area of the center, working status, etc.

Once all the information has been gathered, it should be assessed for the purposes of ACCEPTING or NOT ACCEPTING the communication for processing. This is a decision that will be stated in writing, argued, and, within a time frame of no more than SEVEN days, confirmation of receipt will be communicated to the sender and, where possible, included in the file.

In compliance with Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), Organic Law 7/2021 on the Protection of Personal Data that is

processed for the purposes of Prevention, Detection, Investigation, and Judgment of criminal breaches, and execution of criminal sanctions, the (EU) Directive 2019/1937 relating to the Protection of Personal Data that reports on breaches of EU Law, and the General Data Protection Regulations of the (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND COUNCIL (hereinafter GDPR), the complainant/informant will be informed of the receipt of their communication, its acceptance for processing or its rejection, as well as all the necessary particulars for beginning the investigation (additional information required from them, documentation, etc.).

If the communication contains the personal data of third parties, separate from the party being investigated (for example, witnesses, suppliers, clients, etc.), the Compliance Committee should record, in writing, that the third party should be informed, within a time frame of no more than TEN days, of the circumstances of the communication, and their consent should be requested for processing their personal data.

All these notifications will be decided upon by the Compliance Committee, recorded in the file, in writing, and executed through the communications channel mailbox.

If the Compliance Committee warns that there is an urgent need to inform the appropriate public authority of the facts contained in a communication, they will record this in writing and proceed to inform CRG Management and the Executive, and its governing body without further delay, for subsequent reporting of the facts to the appropriate public authority.

2ND PHASE: INVESTIGATION OF THE COMMUNICATION

In the event that the communication is accepted for processing, and unless commitments lead to a new appointment, the Investigation will be carried out by the Compliance Committee.

In this phase, the PARTY BEING INVESTIGATED and the third parties who are involved (if any) will be notified and INTERVIEWED, so that they can explain and put forward their arguments. Such investigation formalities as are considered necessary will be carried out for both parties, and a documentary record will be made of all actions in the file. In the event that this relates to an issue of scientific malpractice, it shall be as established in the Procedure in cases of suspected CRG scientific malpractice.

The formalities exercised in relation to third parties or other CRG bodies, areas, or departments should be carried out in such a way as to preserve the anonymity of the COMPLAINANT/INFORMANT and the PARTY BEING INVESTIGATED, as well as the reasons for the communication.

During this phase, the Compliance Committee will:

1st.- Investigate the facts which have been communicated, specifically:

- The objective and subjective elements provided by the complainant/informant, prioritizing objective elements that are backed up with documentation that proves the facts communicated, in whole or in part.
- The reputation, trustworthiness, and reliability of the complainant/informant.
- The arguments and defensive evidence provided by the party being investigated.
- The evidence from third parties, or other bodies, areas, or departments of the organization.

2nd.- Analyze and assess the possible consequences that the facts which have been communicated may entail

Firstly, the Compliance Committee should check whether or not these facts occurred as a result of a significant lack of internal controls in CRG. Where necessary, it will propose urgent palliative and preventive measures to avoid further risks.

If the Compliance Committee considers it advisable, it may request Management/the Executive's assistance in the investigation. However, if a member of Management or the Executive was involved in the reported fact, the Compliance Committee will refrain from requesting that this member collaborate.

Secondly, if the seriousness, specialization, or complexity of the facts make it advisable, the Compliance Committee may appoint another responsible person from the management or scientific areas, or a specialist third person, to collaborate in the investigation. If it is possible that assets may be lost as a consequence of the facts that have been communicated, the Compliance Committee should adopt measures aimed at stopping or mitigating said losses or damages. If it is possible that evidence for the investigation may be deleted, the Compliance Committee will be responsible for securing any digital evidence before beginning to investigate the communication.

Lastly, it will check whether it is possible that third parties have suffered damage. In this case, the organization will assess the damage, and the need to inform the third party.

The time frame for carrying out the investigation will depend on the seriousness of the facts that have been communicated, and their potential consequences. The duration of this Phase will remain at the discretion and the risk of the Compliance Committee. Nevertheless, in accordance with that which is established by section 9.1.f) of the (EU) Directive 2019/1937 from the European Parliament and Council of October 23, 2019, relating to the protection of persons who report breaches in EU Law, it should give a response within a reasonable time frame, no longer than three months from the confirmation of receipt, or expiration of the deadline of seven days after the report is made.

3RD PHASE: VERDICT

Following the investigation of the communication, and with the supporting documentation that serves to clarify the facts, the Compliance Committee will prepare a VERDICT, that will contain the following:

- Description of the facts: communication registration number; date of the communication; facts that have been communicated; participating parties; documentation provided throughout the investigation by both parties (complainant/informant and the party being investigated), by other bodies, areas, or departments in the organization, and by third parties; interview with the party being investigated and/or with third parties, etc.
- Analysis and assessment of evidence obtained.
- In the event that the communicated irregularity has indeed been proven, the Compliance Committee will dedicate one section of the verdict to make any Recommendations that it considers necessary to implement in order to improve the internal controls and protocols that were deficient on this occasion.
- Resolution: a resolution will be adopted and, if possible, a response will be provided to the complainant/informant within a reasonable time frame, no longer than three months from the confirmation of receipt of the communication, or expiration of the deadline of seven days after the report is made, as the final result of the investigation needs to be communicated to them. In any case, the resolution that is adopted must be justified, and may consist of:
- I. CLOSURE WITHOUT SANCTION: Following the investigation, it may be decided that the reported breach is manifestly minor, and does not require further follow-up, and so it is CLOSED. Closure is also suitable in cases of repeated reports that do not contain any significant new information on breaches, when compared with a previous report for which the proceedings have been concluded, unless new factual or legal circumstances occur that justify a different follow-up. In these cases, the resolution must be communicated to the complainant/informant, and it must be justified.
- II. CLOSURE WITH SANCTION: the Compliance Committee may propose the application of a sanction, but the decision will fall to CRG management in coordination with the Human Resources and Legal Department, in compliance with the procedures indicated by the application of labor sanctions in the organization.
- III. COMMUNICATION WITH AUTHORITIES: If the communication received seems to relate to the commission of a crime *a priori*, the Compliance Committee should formally report this situation to CRG Management for the purposes of having its report assessed by the appropriate authorities. In this regard, the Spanish Law on Criminal Judgment, section 259, provides that the person who witnesses the commission of any public crime[1]

[1] The classification of a crime as public is linked to the person who is pursuing its prosecution (official or injured party), as **public** crimes can be prosecuted officially without the need for prior reporting by the injured party. In addition to crimes against life and liberty, in the catalog of crimes that entail the criminal responsibility of the legal entity, we have, by way of example, the following public crimes: fraud, bribery, influence peddling, money laundering, financing terrorism, Public Finance and Social Security crimes, environment and

is obliged to immediately bring it to the attention of the Examining Judge, the Justice of the Peace, the Regional or Municipal Judge, or the district attorney closest to their location. They can report it before the Duty Court, the Prosecutor's Office, or at any police station.

- The duty to report certain crimes, which are singled out by criminal legislation, to the appropriate authorities is increased. In this respect, the Spanish Criminal Code, in section 450[2], provides for *"failure in the duty to stop crimes or promote their prosecution"*, sanctioning anyone who does not stop the commission of a crime that affects people's lives, integrity or health, freedom or sexual freedom, if they are able to do so by immediate intervention, and without risk to themselves or others, and anyone who does not go to the authorities, or their officers, if they are able to do so, in order to stop these crimes which they are aware of, and which are about to be committed or currently being committed.
- Date and signature of the Compliance Committee, and of each member of the organization, if they participated.

In all cases, the complainant/informant and the party being investigated will be NOTIFIED of the RESOLUTION. The form of notification will be any valid form (hand delivery, email, bureaufax, etc.) that allows for confirmation of receipt, for the attention of the complainant/informant and the party being investigated.

Once a Resolution on the communication has been adopted, the Compliance Committee will order that it be CLOSED and RECORDING BE LOCKED, for whatever time frame it considers prudent, until such time as it is totally destroyed, in any case, in line with the current legislation in relation to LOPDGDD.

CRG guarantees that any person who, in good faith, makes the organization aware of the commission of a criminal act, collaborates in its investigation, and helps to resolve it, will never be subjected to any reprisals. This guarantee does not cover those who act in bad faith, with the intention of spreading false information or harming others. CRG will adopt the appropriate legal or disciplinary measures to combat this sort of illicit conduct.

natural resources crimes, land use planning crimes, fundamental rights and public freedoms crimes, contraband, among others. On the other hand, **private** crimes are slander and insults between individuals (the law will only be able to intervene once the injured person makes a report or accusation), and **semi-public** crimes may be officially prosecuted once the injured party has initially made the report (crimes of discovery and breaches of confidentiality, intellectual property crimes, assault, harassment, and sexual abuse, among others).

[3] Section 450 of the Spanish Penal Code: "1. The person who, if they are able to do so by immediate intervention, and without risk to themselves or others, does not stop the commission of a crime that affects people's lives, integrity or health, freedom or sexual freedom, will be punished with the **sentence of six months to two years in prison, if the crime was a threat to life, and by a fine of six to twenty-four months in other cases**, unless the crime that they failed to stop corresponds to the same sentence or a lesser one, in which case a lesser sentence than that will be imposed. 2. Anyone who does not go to the authorities, or their officers, if they are able to do so, in order to stop these crimes which they are aware of, and which are about to be committed or currently being committed, will receive the same sentence.

5. Sanctioning System

Once the investigation of the facts has been completed, if it is confirmed that they are true, CRG will take all necessary measures to put an end to the reported act. It will also, if appropriate, and bearing in mind the characteristics of the act, apply the measures it considers suitable in the disciplinary system and in current labor legislation.

The actions that can be imposed internally shall not limit, at any point, the exercise of any legal action that CRG may take.

6. Security and Confidentiality

The electronic communications channel will have an assigned System Administrator in the CRG ICT department. This person is in charge of establishing and customizing the necessary system security, including access restriction, and the ability to lock records which it would need to be impossible to modify once they have been recorded. Special management and administration is established for the deletion of records from the system.

Additionally, the mailbox shall be capable of auditing access to individual records and recording the date, time and username, including any modification of the records.

In order to ensure that the data held is as accurate as possible, any communications that are not relevant, or those for which, once the facts are investigated, it is concluded that they are not accurate or true, shall be immediately deleted.

Likewise, the communications mailbox shall allow the Compliance Committee to store and/or recover key information on each incident, including the date and original source of the communication, the investigation plan, results of interviews or any other procedure from the investigation, pending tasks, final resolution, as well as the chain of custody for any evidence or key information.

Finally, it should be remembered that the confidentiality of the complainant/informant and the person who has been reported shall be maintained at all times, and their identities shall not be revealed outside the scope of the Compliance Committee.

7. Personal data protection

In accordance with that which is explained in this Regulation, please note that personal data provided to CRG by complainants/informants are protected within the framework of reporting, processing, and investigation, and will be deleted once they are no longer necessary and relevant. The personal data related to those reports that are not accepted for processing will be deleted at that point.

The data obtained may be communicated to the appropriate bodies (Security Forces and Bodies of the State, Judges, and Tribunals, etc.) in the event that they confirm the commission of a criminal offense.

At all times, the complainant/informant and the people involved in the commission of the reported acts will have the right to exercise their rights of access, correction, deletion, and opposition, as well as to obtain the limitation of data processing from CRG, where any of the conditions provided for in the data protection regulations is met, and, where appropriate, to request the portability of their data.

8. 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.

9. Related documentation

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

10. Approval of this Regulation

This Communications Channel Regulation has been approved in line with that which is indicated in the history of versions below, and it may be modified in order to maintain the culture of compliance within the organization at all times. This culture of compliance is embodied in the principles of transparency, responsibility, and prudence towards third parties, and towards its own members and business partners.

History of versions:

Version	Date	Approved by	Reason for change
V.1	28/11/2022	Coordinator of the Compliance Committee and Administrative Director of CRG	
V.1	15/12/2022	CRG Board of Trustees	

ANNEX 1: Reporting form

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 whe 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