CRG INTERNAL INFORMATION SYSTEM POLICY

Table of contents

1. Introduction and Objective

The objective of this Policy is to foster and bolster the culture of communication inside the CRG as a tool for preventing and detecting threats to the public interest, guaranteeing and prioritising protection for communicators or informants, pursuant to Law 2/2023 of 20 February, which regulates protection for people who report breaches of the law and the fight against corruption (hereinafter "Law 2/2023, of 20 February"), which transposes, in Spain, the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union Law.

The CRG expects its members to act and perform their functions in accordance with the principle of good faith at all times, which, among other things, calls for constant collaboration with the organisation.

As a tool for the fulfilment of the above, the CRG has activated the following **Internal Information Channel** for the purpose of filing complaints, and which is preferentially available to all employees, researchers, technicians, students, third-party collaborators, suppliers and any other third party via the following email address: compliance@crg.eu or by ordinary mail addressed to the Fundació Centre de Regulació Genòmica, Calle Doctor Aiguader, número 88, Edifici Parc de Recerca Biomédica de Barcelona (PRBB), 08003, for the attention of the Compliance Committee. Informants may also contact the Compliance Committee Coordinator orally, by telephone on their direct number or by means of a face-to-face meeting, submitting their request using one of the aforementioned communication channels. They may also submit notifications or reports anonymously. The Compliance Committee has been appointed by the CRG's Board of Trustees as **Head** of this System, and the Compliance Committee Coordinator is their **Delegated Manager**.

2. Scope

This CRG Internal Information System Policy, applies to and must be enforced by all CRG members.

This Policy has been translated into any languages that may be necessary for all the members of the CRG and any other third parties linked to the organisation to understand its scope and content.

3. On the content of reports

Employees, researchers, technicians, students, collaborating third parties, suppliers and any other third party that engages with the CRG can use this Internal Information System to report, confidentially and anonymously, if they so wish, any breach or omission they learn of and which could involve a breach of European Union Law or their financial interests or criminal or administrative offences within the Spanish legal framework, as well as possible cases of non-fulfilment or breach of the organisation's internal policies.

In this regard, this Internal Information Channel may be used to report actions or omissions that constitute or may constitute offences in the following areas:

- Public provisioning or procurement
- Confidentiality
- Corruption and Fraud
- Competition
- Corporate offences
- Tax and Finance
- Non-fulfilment of the applicable legislation or of Policies, Procedures, Regulations, Protocols, Internal Rules, Code of Conduct or other CRG-specific regulations
- Labour and Workers' Rights
- Environment and sustainability
- Protection from radiation and nuclear security
- Intellectual property and Trade secrets
- Occupational Risk Prevention
- Prevention of Capital Laundering
- Consumer protection
- Personal data protection and privacy
- Public Health and Health Alerts
- Animal food safety, health and welfare
- Network and IT system security
- Product safety and conformity
- Societal
- Others

Furthermore, there is a specific internal information system for eventualities involving the reporting of facts and events related to sexual and or gender harassment, psychological harassment in the workplace or harassment on account of any other difference (such as ethnicity,

religion, disability, etc.). The procedure for receiving and managing such reports is established in the CRG's Protocol for the prevention and management of harassment.

This Internal Information System will be used solely for the purpose described herein and not as a vehicle for organisational complaints.

The internal information channels activated for the receipt of any type of report or information other than the above will not be protected by the scope of protection provided for by this Policy and by Law 2/2023 of 20 February, regulating the protection of people who report breaches of the law and the fight against corruption.

4. On communicators or informants

The principles, guarantees and rights established in this Policy focus on the protection of communicators or informants, prohibiting any type of reprisals and promoting the provision of help and assistance to them.

In this regard, communicators or informants are regarded as all natural persons who report the breaches or offences stated in the preceding section, who are employed in the private or public sector and have obtained information about breaches in their occupational or professional setting, with such cases comprising:

- People in the employment of others, including those whose occupational or professional relationship has concluded.
- Self-employed workers or freelancers.
- Volunteers.
- People on work experience schemes.
- Candidates in a job recruitment process.
- Members of the governing body.
- Anyone working under the supervision of contractors, subcontractors or suppliers for the CRG.

Moreover, the following individuals will also enjoy the protection provided by this Policy in accordance with Law 2/2023 of 20 February:

- workers' legal representatives who are performing advisory and support functions to the informant,
- natural persons who, within the setting of the organisation in which the informant renders services, assist the latter in the process,
- natural persons related to the informant and who may be subject to reprisals (such as the informant's colleagues or relatives) and
- corporate persons for whom the informant works or with whom the latter maintains any other type of relationship in an occupational setting or those in which the informant holds a significant participation. For these purposes, a shareholding in the capital or in voting rights corresponding to shares or interests is regarded as significant when, on account of its or their proportion, the holder is in a position to bring an influence to bear upon the corporate person involved.

5. General principles and guarantees

5.1. INTEGRATION OF INTERNAL CHANNELS

The CRG's Internal Information System, as well as the Internal Information Channel, will be available and accessible to all members or to any third party irrespective of their relationship with the organisation as a comprehensive and preferential information communication channel[1].

5.2. CONFIDENTIALITY and ANONYMITY

The CRG guarantees both the confidentiality and the anonymity of the informant and of any other third party who is or could be mentioned and/or involved in the report in all actions carried out as a result of the report and its subsequent management. Data protection is guaranteed throughout the process, and access by unauthorised personnel during data processing is prevented.

Therefore, the anonymity of the informant and of the person investigated, as well as the reasons for the report, must be safeguarded in the course of all formalities conducted with third parties or with any other CRG area or body.

[1] The guarantees established in this section will be observed and be applicable even when the report is submitted through whistle-blowing channels other than the ones established for this purpose.

The CRG guarantees that the informant's identity may only be disclosed to the Legal Authorities, to the Prosecutor General or to the competent administrative authority as part of a criminal or disciplinary investigation.

Anyone who for different reasons is involved in activities supporting the investigation of a given incident is obliged to treat any information to which they have access with the utmost confidentiality.

In cases in which reports are managed by an external supplier, the latter must demonstrate that they provide adequate guarantees in terms of independence, confidentiality, data protection and secrecy of communication.

If the report is submitted through internal channels other than those established by the CRG or is forwarded to members of personnel who are not responsible for processing it, the aforementioned confidentiality must also be maintained and guaranteed. For this purpose, the CRG promotes the dissemination of and training in this Policy (in accordance with the requirements of art. 9.2.g) of Law 2/2023 of 20 February), with the warning that failure to observe the confidentiality guarantee constitutes a very serious offence of the aforementioned Law and that therefore the recipient of the report must forward it immediately to the Head of the System.

5.3. PRESUMPTION OF INNOCENCE AND HONOUR

The CRG will guarantee the presumption of innocence and respect for the honour of everyone affected by or involved in a report at all times.

Anyone affected by or involved in a report will be entitled to be informed about the actions or omissions attributed to them and also to be heard in the course of the investigation, although under no circumstances will they be informed of the informant's identity.

The CRG will ensure that anyone affected by or involved in the report has the right to the presumption of innocence, the right to defend themselves and the right to have access to the proceedings in the terms regulated in Law 2/2023 of 20 February, as well as to the same protection established for informants, and that their identity will be protected and that confidentiality regarding the facts and the data of the procedure will be ensured.

5.4. ACCESS TO EXTERNAL CHANNELS AND PUBLIC DISCLOSURE

Communicators or informants may submit their report to the Autoridad Independiente de Protección del Informante [Independent Authority for the Protection of Informants] (A.A.I) or to the corresponding authorities or organs in other Autonomous Communities, either directly or after first filing the report through their own Internal Channel.

Moreover, communicators or informants are afforded the possibility of making a public disclosure, which consists of making the information about the facts or events being reported public through this Information System.

In this regard, and for the protection envisaged by Law 2/2023 of 20 February governing people who make public disclosures to be provided, the following conditions must be fulfilled:

a) The person must first have submitted the report through internal and external channels or directly through external channels, without any appropriate measures have been taken in this regard within the established deadline.
b) There must be reasonable grounds to think that either the offence may constitute an imminent or evident danger or threat to the public interest, particularly in a situation of emergency or a risk of irreversible damage, including danger to a person's physical safety; or else, in reports submitted through an external information channel, if there is a risk of reprisals or little likelihood of the information being handled effectively due to the specific circumstances of the case, such as the concealment or destruction of evidence, connivance of an authority with the perpetrator of the offence or the authority is party to the offence.

5.5. PROHIBITION OF REPRISALS

The CRG expressly prohibits any acts that constitute a reprisal, including threats of reprisals and attempted reprisals against anyone who files a report through the Internal Information Channel.

Reprisal is taken to mean any acts or omissions prohibited by law, or which either directly or indirectly constitute unfair treatment placing the people subjected to them at a particular disadvantage with regard to another in their occupational or professional setting, merely for the fact that they are informants or for having made a public disclosure, in accordance with the provisions of article 36 of Law 2/2023 of 20 February.

Any person whose rights are jeopardised or compromised on account of their report or disclosure

after two years have elapsed since the report was filed may request the protection of the competent authority which, in exceptional cases and with justified cause, may prolong the period of protection after giving the people or organs that might have been or be affected a hearing. Any rejection of the extension of the period of protection must be duly reasoned.

5.6. SUPPORT MEASURES

Pursuant to the rules established by Law 2/2023 of 20 February, the CRG, having evaluated the circumstances, will provide the communicator or informant with any ideal support measures that may be necessary.

The foregoing is without prejudice to any assistance that may be applicable pursuant to Law 1/1996 of 10 January, on free legal aid, for the purpose of representation and defence in legal actions resulting from the filing of a report or a public disclosure.

5.7. MEASURES OF PROTECTION FROM REPRISALS: RELEASE FROM RESPONSIBILITY

Any person who submits information through the Internal Information System and its Internal Information Channel will not be regarded as having breached any restriction on the disclosure of information and nor will they be liable or responsible for any such disclosure provided that they had reasonable grounds to believe that such a report or, as the case may b, public disclosure, was necessary to reveal an action or omission pursuant to this Policy.

Informants will not be liable or responsible with regard to the acquisition of or access to information reported or disclosed publicly provided that any such acquisition or access does not constitute an offence.

5.8. PERSONAL DATA PROTECTION

The CRG undertakes to process the data contained in the report in full compliance with the legislation governing the protection of personal data and informants.

Any personal data processing resulting from the application of Law 2/2023 of 20 February, on which this Policy is based, will be governed by the provisions of Title IV of the aforementioned Law, the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), the Spanish Organic Law 3/2018 of 5 December on Personal Data Protection and the Guarantee of Digital Rights and the Spanish Organic Law 7/2021 of 26 May on the protection of

personal data processed for the purpose of prevention, detection, investigation and prosecution of criminal offences and the enforcement of penalties for criminal offences.

No personal data not patently relevant to the processing of a specific item of information will be collected or, if it is collected accidentally will be deleted without undue delay.

6. Compliance commitments

All people who engage with the CRG must be conversant with the ethical and legal principles applicable to their roles and functions, as well as with all the provisions and obligations contained in the different control measures implemented by the CRG, and undertake to fulfil them and to maintain its integrity and reputation.

This Policy, together with the Internal Information Channel Regulations and other in-house policies and rules implemented by the CRG, constitute the cornerstone of the organisation's compliance culture. For this reason, compliance with this Policy is mandatory for anyone linked to the CRG, and therefore not only is compliance with the applicable legislation demanded, but so too is the upholding of the organisation's values and ethical and responsible principles.

This Policy is made available to all members of the CRG and any other stakeholders to ensure that they will be conversant with it.

7. Disciplinary System

Any action that could constitute a limitation of informants' rights and guarantees or of their confidentiality and anonymity, a breach of the obligation to keep all information received and the data contained in it secret, may constitute a serious or very serious offence in terms of non-fulfilment of the provisions of Law 2/2023 of 20 February regulating the protection of people who report breaches of the law and the fight against corruption.

8. Responsibility and Oversight

The Compliance Committee is the organ responsible for this Internal Information System and is tasked with overseeing that it operates properly and that all reports received are managed with the requisite diligence. It will also have powers for managing the system and for processing

investigation reports or proceedings.

This collegiate organ appoints the Delegated Manager, namely the Compliance Committee Coordinator, to manage the system and to handle investigation proceedings or formalities (**Annex 1** of this document).

The Delegated Manager will enjoy independence and autonomy in the performance of their functions and will have been duly appointed by the CRG's governing body. The competent authority in these matters will be notified of this appointment in the form and within the term provided for by the Law.

This Policy will be reviewed and/or amended by the Head of the Internal Information System, who may outsource the service to specialised professionals:

1. Whenever relevant changes take place in the organisation, control structure or professional activity of the CRG that render such a course of action advisable.
2. Whenever legal amendments are implemented and render this advisable, and/or for the purpose of improving confidentiality and the effective management of any reports submitted.
3. Whenever any relevant offences against or breaches of the Policy's provisions are committed that also render such a course of action advisable.

This Policy will be reviewed periodically, every two years at least, even if none of the aforementioned circumstances occur.

9. Version History

Version	Date	Approved by	Reason for the change
v.1	29/11/2024	Compliance Committee Coordinator and Administrative Director of the CRG	Division of the Internal Information Channel and creation of this Internal Information System Policy in fulfilment of Law 2/2023 of 20 February, regulating the protection of people who report breaches of the law and the fight against corruption.
	19/12/2024	CRG Board of Trustees	

10. Annexes

Annex 1: Compliance Committee/Head of the CRG's Internal Information System:

MEMBERS OF THE COMPLIANCE COMMITTEE AND DELEGATED MANAGER OF THE INTERNAL INFORMATION SYSTEM (IIS)
Compliance Committee Coordinator and Delegated Manager of the IIS: Head of Legal Assessment
Senior People Department representative: People Senior Administrator
Senior Representative Finance Department: Controller
System Delegated Manager: Administrative Director of the CRG