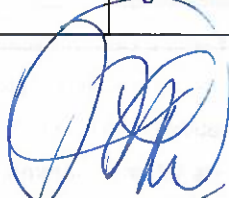
	<b>Internal Information System</b>	
Date: November 2023	Edition: 1	Page 1 of 19
<div> <div>           Approved By:            Sole Administrator         </div>  </div>		

## Internal Information System Policy

### (Ethics Channel & Other Communication Channels)

---

<b>Index</b>	
<b>Internal Information System</b>	<b>1</b>
1. Purpose of the Policy	3
2. Scope of Application	3
3. Submitting a Communication	3
3.1 How can I submit a <i>Communication</i> ?	3
3.3 What Happens in Emergency Cases?	5
3.4 What Information do I Need to Provide When Making a <i>Complaint</i> ?	5
3.5 What Happens When a Communication is Made Through the Ethics Channel?	5
4. Principles & Guarantees of the Internal Information System	6
5. Protection of the Parties Involved in a <i>Complaint</i>	8
5.1 Scope of Protection	8
5.2. Protection & Support Measures	8
5.2.1. Protection & Support Measures for the <i>Whistleblower &amp; Relevant Interested Parties</i>	8
5.2.2. Protection Measures for the <i>Respondent</i>	8
5.3. Activation of Protection	9
6. Fraudulent or Bad Faith Complaints	9
7. Roles & Responsibilities	9
7.1. Compliance Committee	9
7.2. Governing Bodies	9
8. Protection of Personal Data	10
8.1. Preservation of Information	11
8.2. Rights of the <i>Whistleblower, Respondent &amp; any Relevant Interested Party</i> , in Matters of Data Protection	11
<b>Annex I</b>	<b>13</b>
Definitions	13
<b>Annex II</b>	<b>15</b>
Examples of Possible <i>Retaliation and Harmful Conduct</i>	15
<b>Annex III</b>	<b>16</b>
Examples of Protections and Support Measures	16
<b>Annex IV</b>	<b>17</b>
Measures Applicable to IRIDIUM & Its Subsidiaries Located in the European Union	17
<b>Annex V</b>	<b>18</b>
Measures Applicable to IRIDIUM Subsidiaries in Latin America	18
Communication Channels	18
<b>Annex VI</b>	<b>19</b>
Measures Applicable to IRIDIUM Subsidiaries in North America	19
Communication Channels	19

## 1. Purpose of the Policy

The purpose of the Internal Information System Policy (the "**Policy**"), approved by *IRIDIUM Group's Administrative Body*, is to establish the framework for the use and management of the different *Communication* channels existing in *IRIDIUM Group*, through which *IRIDIUM Group Members*, *Business Partners* and *Third Parties* may submit *Inquiries* and/or *Complaints* that may arise within *IRIDIUM Group* during its activities.

This *Policy* details the different channels in the internal reporting system which can be used to submit *Inquiries* and/or *Complaints*, including, among others, notifying a supervisor who must then communicate it to the *Compliance Committee* or general *Communications* through the Ethics Channel.

All *IRIDIUM Group Members* have the obligation to report individual or collective behaviors that may imply a breach of the contents of this *Policy* or the other documents that make up *IRIDIUM Group's Criminal Compliance and Anti-Bribery Management Systems (the "Systems")*, regardless of whether such behaviors have been ordered or requested by a supervisor.

The purpose of this *Policy*, which sets forth guidelines and details the use the Ethics Channel, is to provide advice, certainty and protection to persons made aware of existing or potential *Violations*. *IRIDIUM Group* wishes to emphasize that, in any case, *Retaliation* and other *Harmful Conduct* against *Whistleblowers* for having filed an *Inquiry* and/or *Complaint* are strictly prohibited.

**Annexes I and IV** of this *Policy* contain additional defined terms of this document.

## 2. Scope of Application

This *Policy* is mandatory for *IRIDIUM Group*. *IRIDIUM Group* will endeavor to ensure that the principles set forth in this *Policy* also apply to non-controlled interests and joint ventures of *IRIDIUM Group*.

*IRIDIUM Group Members* shall comply with the *Policy's* contents, regardless of their position and function. The scope of this *Policy* covers all *Inquiries* and *Complaints* that may be raised by any *IRIDIUM Group Member*, *Business Partners* and/or *Third Parties*.

This *Policy* also applies to those individuals who, though not *IRIDIUM Group Members*, have knowledge of the existence of any *Violation* in their professional relationship with *IRIDIUM Group*.

The *Complaints* received may concern any *Violation* the *Whistleblower* believes may be applicable to *IRIDIUM Group*, as well as any document that integrates *IRIDIUM Group's Systems*.

## 3. Submitting a Communication

### 3.1 How can I submit a *Communication*?

*IRIDIUM Group Members*, *Business Partners* and *Third Parties* are provided with different internal channels so that they can submit any type of *Inquiry* and/or *Complaint*.

In particular, the following written *Communication* channels are available:

- The Ethics Channel accessible through the corporate website: <https://www.IRIDIUMconcesiones.com/compliance/canal-ético/> or directly through the following link: [IRIDIUMacsinfra.ethicspoint.com](mailto:IRIDIUMacsinfra.ethicspoint.com)
- By mail to the following address:

Canal Ético IRIDIUM Concesiones de Infraestructuras SA  
Avda. del Camino de Santiago 50, 28050,  
Las Tablas, Madrid, Spain

In case of *Complaints* or *Inquiries* made by *IRIDIUM Group Members*, it will also be possible to submit a written *Communication* by e-mail or a verbal *Communication* to:

- The *Whistleblower's* supervisor or a member of the *Administrative Body* for the relevant *IRIDIUM Group* entity (who must inform the *IRIDIUM Compliance Committee* or the *IRIDIUM Group Compliance Committee*, who is available to receive the *Complaint* or *Inquiry*);
- Any member of the *IRIDIUM Compliance Committee*, or of the relevant *IRIDIUM Group Compliance Committee* who is available to receive the *Complaint* or *Inquiry*;
- *IRIDIUM* compliance department

Finally, in the case of *Complaints*, it shall also be possible for the *Whistleblower* to request a face-to-face or videoconference meeting with the *Compliance Committee*, or with any of its members, which shall take place within seven (7) days from the request for the meeting.

Regardless of the means of *Communication* used, the *Whistleblower* may designate a preferred means of *Communication* to receive information on the status of his/her *Complaint* or to be contacted for additional information and/or clarification.

All *IRIDIUM Group Members* and anyone else who suspects or knows of any *Violations* related to *IRIDIUM Group* are encouraged to use these internal channels to submit their *Complaints*.

All *Complaints* shall be handled by the *Compliance Committee* under the terms described in this *Policy* and developed in the *Non-Compliance and Complaint Investigation Procedure*.

In addition, any potential *Whistleblower* from the European Union is informed that it also has external reporting channels that can be used to contact the appropriate authorities and, where appropriate, to the institutions, bodies, or agencies of the European Union, such as, among others:

- In matters related to securities markets: [Complaint form \(cnmv.es\)](#).
- In antitrust matters: [Complaint of prohibited conduct | CNMC](#).
- In the area of money laundering: [Communication by indication | Sepblac](#).
- In matters of tax violations: [Tax Agency: Complaints](#).
- Fraud and irregularities related to European funds: [Anti-fraud Mailbox](#)
- Recovery and Resilience Mechanism Complaints Channel - Recovery, Transformation and Resilience Plan Recovery, Transformation and Resilience Plan Government of Spain. ([planderecuperacion.gob.es](#)).

Potential *Whistleblowers* in the European Union are also informed of the existence of a public body called the *Independent Authority for Whistleblower Protection*, to which they can also turn.

The *Whistleblower* reporting a *Complaint* must collaborate with the *Compliance Committee* in the analysis and investigation phase when so required. The *Whistleblower* and *IRIDIUM Group* must both maintain confidentiality regarding the cooperation provided and the allegations brought forth.

### 3.2 When to Report?

*IRIDIUM Group* considers it important to promote an environment where people feel comfortable reporting any incident that violates *IRIDIUM Group's* Code of Conduct, *Systems* and, therefore, encourages an environment in which people can report allegations related to possible *Violations*.

The above must be in line with a principle that governs all *IRIDIUM Group's* relations with its stakeholders: *Complaints* must always be made in good faith. This means that, at the time of the *Complaint*, the *Whistleblower* must have reasonable knowledge that the information he or she is reporting is true and presents possible violations.

### 3.3 What Happens in Emergency Cases?

The processing of a *Complaint* submitted through the different channels available to *IRIDIUM Group* requires that the applicable *Compliance Committee* classify the *Complaint* internally for appropriate processing. The parameters being set forth in the *Non-Compliance and Complaint Investigation Procedure*.

In any case, it is mandatory to immediately notify a supervisor and/or the applicable *Compliance Committee* to address ethical issues that arise as efficiently as possible, in compliance with applicable laws and regulations and in accordance with the *IRIDIUM Group's Non-Compliance and Complaint Investigation Procedure*.

### 3.4 What Information do I Need to Provide When Making a Complaint?

It is recommended that the *Whistleblower* provide all the information he/she is aware of in connection with the possible *Violations* and that he/she does so in detail. In addition, it is preferable that any evidence or documents in support of the *Complaint* be provided or clearly referenced in the *Complaint*. This allows the case to be handled as quickly and efficiently as possible. It must be noted that only evidence which the *Whistleblower* can verify has been obtained in a lawful manner, without violating the rights of those involved in the *Complaint* or of *Third Parties* should be provided.

### 3.5 What Happens When a Communication is Made Through the Ethics Channel?

*Communications* through the Ethics Channel are stored directly on a digital platform, which is highly secure.

The Ethics Channel allows the *Whistleblower* to specify the place, date or company affected, as well as the persons related to the *Complaint*. It also allows the *Whistleblower* to opt for anonymous *Communication*.

The platform will give the *Whistleblower* the option to attach to the *Complaint* supporting documentation that substantiates the *Complaint's* contents. Only documentation obtained in a lawful manner must be provided.

In the case of filing a *Complaint* through the Ethics Channel, the platform will provide the *Whistleblower* with a case number, as well as a password for his or her exclusive use. With this case number and password, the *Whistleblower* will be able to log in to the platform to obtain comments and/or updates on his/her *Complaint*. The *Ethics Channel* will allow the *Whistleblower* to provide



additional information to modify or supplement his or her report. In addition, it allows you to file a report anonymously.

The principle of action is that, when the *Communication* indicates a possible *Breach*, an investigation will be initiated in accordance with the *Complaint and Non-compliance Investigation Procedure*.

## 4. Principles & Guarantees of the Internal Information System

Regarding the *Complaints* made by *IRIDIUM Group Members, Business Partners* and *Third Parties, Retaliation* and other *Harmful Conduct*, discrimination or sanctions for those *Communications* made in good faith or for those actions aimed at avoiding participation in unlawful actions is prohibited.

In any case, the management of *Complaints* within the *Internal Information System* shall be always guided by the following three general principles:

**Principle of Confidentiality:** Any person participating in the investigations must maintain the confidentiality of the information received through the Ethics Channel or any known information and may not disclose to *Third Parties* the information known in the exercise of their functions, especially that which relates to personal data.

Notwithstanding the foregoing, in the event there is the need to share information with the parties involved in the case, those persons participating in the investigation shall provide a minimum amount of information and on a need-to-know basis only in those cases where the information is strictly necessary.

If in a particular case, it is necessary for a person from another department to join the investigation process, he/she will be informed of the confidentiality obligations as well. Depending on the type of case, the signing of an agreement to emphasize the importance of confidentiality may be considered.

**Principle of Objectivity:** All facts and circumstances surrounding any allegations against a *Respondent* will be investigated, including those that exempt, extinguish, or mitigate them.

Investigators must ensure that they remain objective during the investigation; and

**Principle of Impartiality:** Investigators must ensure that they are impartial throughout the investigation and that they have no personal ties to the *Respondent* that might impair their impartiality or any interest in the outcome.

In addition to the foregoing and during the management of the *Complaints*, Investigators must also adhere to the following principles:

- **Principle of Adequacy and Sufficiency:** *IRIDIUM Group* will assign any necessary resources to the investigation necessary resources to ensure an appropriate resolution. *IRIDIUM Group's* deliberation process must be traceable to justify the measure, if necessary, to any *Third Party*.
- **Principle of Proportionality and Subsidiarity:** This principle responds to the need for any sanctions imposed to be set in accordance with the severity of findings, preventing it from being an arbitrary or disproportionate measure. For such purposes, the following principles shall be considered:
  - Adequacy: Sanctions must be appropriate to the purpose they justify.

- Sufficiency: Sanctions must be sufficient for their intended purpose.
- Due process: Every person has the right to be heard and to assert his or her legitimate claims against those in charge of the investigation.

Likewise, the least burdensome consequence will be considered according to the circumstances of the case.

- **Principle of Presumption of Innocence:** A *Respondent* has the right to be treated as if he/she is innocent until, if applicable, the existence of a *Violation* is proven, and a sanction is imposed.
- **Principle of compliance with applicable regulations:** The commitment to ethical principles engrained into the corporate culture would be undermined if the methods used were unlawful. *IRIDIUM Group* expresses a commitment to respect the rights of affected persons to be heard and to provide information to those affected. The persons denounced for allegations that may be under investigation shall have the right to defend himself/herself against any such allegations.
- **Protection of Whistleblowers in good faith:** *IRIDIUM Group* ensures the protection of its *Whistleblowers*. As a general principle, their identity will not be disclosed beyond the key personnel designated to the investigation and management of the cases, without the explicit and unequivocal consent of the *Whistleblower*.

*IRIDIUM Group* does not tolerate any *Retaliation* or *Harmful Conduct* -by action or omission regardless of whether it is inside or outside of the workplace, against anyone who communicates information that may constitute a *Violation* in accordance with the provisions of this *Policy*, and will provide protection and support, as needed, from the time of filing the *Complaint*.

This protection shall also apply to the *Respondent* and any other *Relevant Interested Party* throughout the *Complaint* process, such as a family member or partner.

*IRIDIUM Group* will not discriminate against any person based on the *Complaint*, nor shall it engage in *Retaliation*, *Harmful Conduct*, or intimidation of any kind against them.

*Violations* of the above principles shall be investigated and, where appropriate, sanctions shall be adopted in accordance with applicable legislation. Further, provisional measures may be adopted while sanctions are pending, including but not limited to the separation of persons in the workplace, or any other measure deemed appropriate under the circumstances.

Any protection measure is subject to the *Whistleblower's* allegations being made in good faith and with the reasonable belief that the information he/she is providing is truthful. *Whistleblowers* shall not be deemed to have breached any confidentiality restrictions on the acquisition, access, or disclosure of *IRIDIUM Group* information, and shall not incur any liability of any kind provided that:

- a) they act in good faith; and
- b) the access or acquisition of information provided does not in itself constitute a criminal *Violation*.

The protection guaranteed by this procedure extends to the *Relevant Interested Parties*, among others, to co-workers, family members, witnesses or Third Parties who intervene for the best

resolution of the case. Such individuals shall also be required to observe the duty of confidentiality, if applicable.

## 5. Protection of the Parties Involved in a *Complaint*

*IRIDIUM Group* will provide protection and support to both the bona fide *Whistleblower* and the *Relevant Interested Parties* against the possible harm they may suffer from reporting possible *Violations* of which they have become aware, under the terms contemplated in section 5.2.1 of this *Policy*.

### 5.1 Scope of Protection

*The protection of Whistleblowers and Relevant Interested Parties shall extend to all Retaliation and other Harmful Conduct to Whistleblowers.*

*Retaliation and other Harmful Conduct may involve any action or omission, whether attempted, threatened or materialized, direct or indirect, from which harm may result, either professionally or personally.*

*Several examples of possible Retaliation and Harmful Conduct are attached as **Annex II** to this Policy.*

### 5.2. Protection & Support Measures

#### 5.2.1. Protection & Support Measures for the *Whistleblower & Relevant Interested Parties*

Protection shall involve taking reasonable steps to prevent harm to and jeopardizing the confidentiality of the *Whistleblower* or the *Relevant Interested Parties*. These measures may be of a psychological, financial, legal, or reputational nature.

For its part, support will involve encouraging and reassuring the *Whistleblower* or *Relevant Interested Parties* of the value of reporting *Violations* and taking steps to assist in their welfare.

The *Compliance Committee* shall be responsible for ensuring that such support and protection measures are implemented in *IRIDIUM Group*.

On the other hand, if *IRIDIUM Group* becomes aware that *Harmful Conduct* is being or has been carried out, appropriate measures will be taken to stop such conduct.

A set of measures for the protection of the *Whistleblower* and other *Relevant Interested Parties* is attached as **Annex III** to this *Policy*. **Annex IV** contains additional *Whistleblower* and other *Relevant Interested Parties'* protection measures provided by the *Independent Authority for Whistleblower Protection* applicable exclusively to *IRIDIUM* and its European subsidiaries.

#### 5.2.2. Protection Measures for the *Respondent*

Similarly, *IRIDIUM Group* affords different protection measures for the *Respondent*.

In this regard, *IRIDIUM Group* will ensure:

- To maintain the confidentiality of the identity of the *Respondent*, as well as the commitment to protect it throughout the procedure.
- To prevent the *Respondent* from being exposed to reputational damage or other negative consequences during the investigation.



- To ensure the *Respondent's* right to defend against any allegations of *Violation(s)*, including but not limited to the right to be heard, the possibility of presenting allegations, and providing the evidence he/she considers pertinent to defend him/herself.
- To allow the *Respondent* to have access to the file to be aware of the actions or omissions attributed to him/her and to be informed of the processing of his/her data protection rights.
- If evidence of *Violations* is not obtained, adopt additional remediation measures.

### 5.3. Activation of Protection

The protection and support provided to the *Whistleblower*, other *Relevant Interested Parties* and *Respondents* will be triggered and initiated as soon as a *Complaint* is received and will continue during and after the conclusion of the investigation process.

## 6. Fraudulent or Bad Faith Complaints

The protection and support provided by *IRIDIUM Group* will be subject to the *Whistleblower* having filed the *Complaint* acting in good faith.

The *Whistleblower* must have reasonable grounds to believe, considering the circumstances and the information available to him/her, that the information he/she reports is true. In this sense, good faith implies having, at least, reasonable grounds to believe that the information on possible *Violations* reported was true at the time of reporting.

Those who deliberately and knowingly communicate incorrect or misleading information will not be afforded protection. In addition, *IRIDIUM Group* will analyze each specific case for the purpose of imposing proportionate disciplinary measures against its *IRIDIUM Group Members* or commercial measures against *Business Partners* and *Third Parties* who file a bad faith *Complaint*.

## 7. Roles & Responsibilities

### 7.1. Compliance Committee

In the case of *IRIDIUM* and its European subsidiaries, the *IRIDIUM Compliance Committee* has been appointed by its *Administrative Body* as the head of the *Internal Information System* in accordance with the provisions of this *Policy*, with the *Head of Compliance* appointed as representative before the *Independent Authority for the Protection of Whistleblowers*.

The roles and responsibilities of the different *Compliance Committees* in relation to *Complaints* are described in the *Non-Compliance and Complaint Investigation Procedure*.

### 7.2. Governing Bodies

*IRIDIUM's Administrative Body* shall be responsible for:

- Formally approving this *Policy*, as well as any modifications or updates that may be necessary to maintain its validity and effectiveness.
- Approving the *Non-Compliance and Complaint Investigation Procedure*, as well as any modifications or updates that may be necessary to maintain its validity and effectiveness.
- Designating the person in charge of the *Internal Information System* for the *Systems* that require it, in accordance with the provisions and regulations of Law 2/2023 for the management of *Communications* related to *Violations*.

In addition, the *IRIDIUM Group's Administrative Body* is responsible for adopting the relevant decisions regarding the *Complaints* once it has received the investigation report and conclusions drawn up by the relevant *IRIDIUM Group Compliance Committee*.

The *Administrative Body* of *IRIDIUM Group* shall inform the relevant *Compliance Committee* of *IRIDIUM Group* of the actions agreed or ratified, so that they are duly documented and recorded. Among others, it shall establish disciplinary measures that are legitimate and proportionate to the *Violation*, and the relevant *Compliance Committee* shall inform the corresponding supervisor, as necessary.

## 8. Protection of Personal Data

*IRIDIUM Group* will treat the data received through the *Internal Information System* in accordance with current data protection regulations.

*IRIDIUM Group* is committed to maintaining strict protection of privacy, security, and data preservation, as detailed in the *Compliance* policies and procedures. These rules will also apply with respect to all personal data related to *Complaints* made in accordance with this *Policy*.

The processing of personal data will be for the purpose of managing and resolving any *Inquiry* or *Complaint*, as well as to analyze the criticality of the allegations reported, to carry out an investigation into possible *Violations*, to adopt the necessary precautionary measures and, if necessary, to initiate the corresponding internal or legal actions.

To fulfill these purposes, certain personal data and information must be collected, either directly from the *Whistleblower*, from the *Relevant Interested Parties*, through the person/s determined by *IRIDIUM Group* or through authorized *Third Parties* specifically contracted for such purposes, who will guarantee the highest level of confidentiality and technical security.

All *IRIDIUM Group Members* are obliged, especially within the scope of the Ethics Channel, to provide true, truthful, and lawful information, being solely responsible for any false or inaccurate statements they provide, as well as for the internal, administrative and/or legal consequences that may apply.

*Iridium Group* shall ensure in all cases that the different channels of *Communication* with the *Compliance Committee* constitute a secure medium, equipped with the measures required by the regulations on personal data protection and information security.

In any case, it will be guaranteed that no personal data is collected from those *Whistleblowers* who wish to formalize their *Communications* anonymously.

Access to personal data shall be limited, within the scope of its competences and functions, exclusively to:

- a) The *Head of Compliance* and whoever manages it directly in accordance with the provisions of this *Policy*.
- b) The head of Human Resources of *IRIDIUM Group* or the duly designated competent body, only when disciplinary measures may be taken against an employee.
- c) The person in charge of *IRIDIUM Group's* legal services, should it be necessary to take legal action in relation to the facts described in the *Communication*.
- d) Data processors are involved in the processing of data, with the appropriate safeguards in

- accordance with data protection regulations.  
e) *IRIDIUM's* Data Protection Officer.

### 8.1. Preservation of Information

*IRIDIUM Group* will treat, manage, and keep the information and personal data contained in the *Complaints*, investigations, reports, and other documentation in accordance with the terms established in the current regulations on personal data protection and other applicable regulations. This information will also be kept under the custody of the *relevant Compliance Committee* and will be deleted, blocked, or anonymized at the end of the legal deadlines.

*IRIDIUM Group* will keep a record of all *Complaints* received. These records and the personal data they contain will be kept confidential. Records shall not be retained longer than necessary and in any event for as long as necessary to comply with any applicable legal requirements from time to time.

personal data that is subject to processing may be kept only for the time necessary to decide on the appropriateness of initiating an investigation into the allegations reported and, at the most, up to three months from their registration without having initiated investigation actions, at which time they must be deleted, unless the purpose of retention is required by law or in accordance with internal recordkeeping policies and procedures. *Communications* that have not been acted upon may only be recorded in anonymized form.

If necessary to investigate the allegations, personal data may be processed outside the *Ethics Channel* for the time necessary to reach a decision, provided that reasonable security measures and confidentiality obligations are observed. Once the investigation has been completed and the appropriate actions have been taken, as the case may be, the data in those *Complaints* that have been processed will be redacted to comply with the corresponding legal obligations in each case.

If it is decided not to investigate a *Complaint* filed, the information may be kept in an anonymized form.

If it is proven that all or part of the information provided is not truthful, it will be immediately deleted, unless such lack of truthfulness may constitute a criminal offense, in which case the information will be kept for the time necessary for applicable criminal and legal proceedings.

### 8.2. Rights of the *Whistleblower*, the *Respondent* & any *Relevant Interested Party*, in Matters of Data Protection

The *Whistleblower* may exercise, at any time and under the terms provided for by the applicable regulations, access to personal data concerning him/her. If this person believes that the data is incorrect or incomplete, he/she may request its rectification in accordance with the applicable legislation. They may also request the deletion of data if it is no longer needed, except where there is a legal obligation to retain it or that the processing of their personal data be restricted and may object to the processing of their personal data. At the time of filing the *Complaint* the *Whistleblower* will be informed as to how he/she can exercise all these rights and at any time they can request access to their personal data to obtain the relevant information they are interested in.

*Whistleblowers* may also file a *Complaint* with the competent data protection authority if they deem it appropriate.

The *Respondent* and any *Relevant Interested Party* shall have the same data protection rights as the

*Whistleblower*, with the following exceptions:

- The *Respondent* will be informed about the processing of his/her data at the time he/she is notified, if applicable, of the *Communication* received concerning him/her.
- *Relevant Interested Parties* will be informed about the processing of their data at the time of their first interaction if they have not already been informed previously.
- If the *Respondent* exercises the right to object, it will be presumed that, unless there is evidence to the contrary, there are compelling legitimate reasons that legitimize the processing of his or her personal data.

### **8.3 More Information About the Treatment of Personal Data**

Individuals may obtain further information about the processing of their personal data and the contact details of the entity's possible representative for this purpose, as well as of the Data Protection Officer or other person responsible for privacy matters.

## Annex I

### Definitions

Defined terms (in *italics*) used in the *Policy* shall have the meanings set forth below:

**Administrative Body:** The governing body of *IRIDIUM* or any of its subsidiaries, as applicable, to the extent that it is assigned the fundamental responsibility and authority for activities, governance, and policies.

**Business Partners:** Any legal or natural person, except *IRIDIUM Group Members*, with whom *IRIDIUM Group* maintains or plans to establish some type of business relationship. By way of example, but not limited to, external advisors, *joint ventures* or individuals or legal entities contracted by *IRIDIUM Group* for the delivery of goods or provision of services are included.

**Communication:** A statement that records a question about the scope, interpretation, or compliance with the regulations applicable to the *IRIDIUM Group*. Depending on its content, a communication may consist of an *Inquiry* or a *Complaint*.

**Complaint:** *Communication* regarding a possible *Violation* (active or omissive behavior) of the regulations applicable to *IRIDIUM Group*, understood as the set of ethical commitments and compliance voluntarily assumed by *IRIDIUM Group*, as well as the legislation in force that is always applicable.

**Compliance Committee:** Each of the *IRIDIUM Group's* compliance committees selected to deal with the *Inquiry* and/or *Complaint*, as the case may be, which has been endowed with autonomous powers of initiative and control, and is entrusted, among other duties, with the responsibility of supervising the operation and observance of the *IRIDIUM Group's Systems*.

**Harmful Conduct:** Any act or omission, whether attempted, threatened, or actual, direct, or indirect, intentional, or negligent, that may result in harm or disadvantage to the *Whistleblower* or other *Relevant Interested Parties*, both in the workplace and in the personal sphere, solely because of their status in relation to the *Whistleblower* or because they have made a public disclosure.

**Head of Compliance:** The person responsible for the compliance department in each of *IRIDIUM Group's Systems*, and who has access to the Ethics Channel.

**Inquiry:** *Communication* by which any *IRIDIUM Group Member* requests a clarification, response or opinion on the scope, interpretation, or compliance with the regulations applicable to the *IRIDIUM Group*.

**Internal Information System:** System of the different communication channels existing in *IRIDIUM Group*, through which *IRIDIUM Group Members*, *Business Partners* and *Third Parties* can submit *Communications*, including *Complaints* or *Inquiries*, to *IRIDIUM Group*.

**IRIDIUM:** Iridium Concesiones de Infraestructuras S.A

**IRIDIUM Group:** *IRIDIUM* or its subsidiaries, including ACS Infrastructure Development, Inc., and ACS Infrastructure Canada Inc.

**IRIDIUM Group Member/Members:** The members of the *Administrative Body*, management personnel and employees of *IRIDIUM Group*.



**Non-Compliance and Complaint Investigation Procedure:** Document that establishes the necessary mechanisms for the early *Communication* and management of any *Violation*, as well as the necessary procedures for the processing and internal investigation of those *Complaints* or any known circumstance that should be investigated.

**Relevant Interested Parties:** A party that can affect, be affected by, or perceive itself to be affected by the *Complaint*. This includes the following:

- Witnesses, or other people involved in the *Complaint*.
- Investigators,
- family members, union representatives, and other people supporting the *Whistleblower*.
- Those from which the information that motivated the filing of a *Complaint* is obtained.

**Respondent:** Natural or legal person(s) linked to the reported violations, as perpetrators, participants or even accessories. They may be identified in the *Complaint* or within the subject of the *Inquiry*.

**Retaliation:** Any action or omission, whether attempted, threatened, or actual, direct, or indirect, that may result in harm or disadvantage to the *Whistleblower* or other *Relevant Interested Parties*, in the work or professional sphere, solely because of their status in connection with the *Complaint* or because they have made a public disclosure.

**Third Party:** Natural or legal person or body independent from *IRIDIUM Group*.

**Violation:** Behavior, active or omissive, that involves the violation of applicable laws and/or regulations applicable to the *IRIDIUM Group*, including, among others and when relevant, any violation of European regulations and/or serious or very serious criminal, administrative or labor violations relating to occupational health and safety at work, established in the Spanish legal system, occurring within the *IRIDIUM Group*. A violation, depending on its seriousness, may range from a mere formal violation of a requirement included in an internal rule, to the commission of acts constituting a crime potentially attributable to *IRIDIUM Group*.

**Whistleblower:** Person or entity that files a *Complaint*, including:

- *IRIDIUM Group Members*
- *Business Partners*
- *Third Parties* and other individuals such as, for example, labor union representatives
- Any person or entity within the above contexts

## Annex II

### Examples of Possible *Retaliation* and *Harmful Conduct*

The following are some behaviors that may be considered as *Retaliation* or *Harmful Conduct*:

- Dismissal, suspension, removal, or equivalent measures.
- Early termination or cancellation of contracts for goods or services.
- Non-renewal or early termination of a temporary employment contract.
- Change of job position or duties, change of work location, reduction in salary or change in working hours or other working conditions.
- Demotion or denial of promotion.
- Imposition of any disciplinary measure, reprimand, or other sanction, including monetary sanctions.
- Denial of services.
- Denial of training.
- Damage, including to your reputation, especially on social media, or economic loss, including loss of business and revenue.
- Any type of act, intentional or reckless, that causes harm, physical or psychological.
- Medical or psychiatric referrals.
- Negative performance evaluation or adverse references regarding your employment.
- Coercion, intimidation, harassment, ostracism, or isolation.
- Discrimination, unfavorable or unfair treatment.
- Blacklisting from a project, which may imply that in the future the person will not find employment in that sector.
- Disclosure of the *Whistleblower's* identity.
- Financial loss.
- Cancellation of a license or permit.

## Annex III

### Examples of Protections and Support Measures

If *Whistleblowers* and other *Relevant Interested Parties* may be subject to any *Retaliation or Harmful Conduct*, the protective measures may be invoked to:

- Reinstatement the *Whistleblower* or *Relevant Interested Party* in the same or equivalent position, with equal salary, responsibilities, job position and reputation.
- Enable equitable access to promotion, training, opportunities, benefits, and rights.
- Restore the *Whistleblower* or *Relevant Interested Party* to the previous commercial position in relation to *IRIDIUM GROUP*, if applicable.
- Withdraw litigation.
- Apologize for any damage suffered.
- Grant compensation for damages.

## Annex IV

### Measures Applicable to IRIDIUM & Its Subsidiaries Located in the European Union

#### Definitions

**Retaliation:** Any action or omission, whether attempted, threatened, or actual, direct, or indirect, that may result in harm or disadvantage to the *Whistleblower* or other *Relevant Interested Parties*, in the work or professional sphere, solely because of their status in connection with the *Complaint* or because they have made a public disclosure.

*IRIDIUM* and its subsidiaries located in the European Union guarantee the necessary protection and support from the moment the *Complaint* is filed until two years after the end of the investigation. However, after the two-year period has elapsed, the *Whistleblower* may request the protection of the *Independent Authority for Whistleblower Protection* which, exceptionally and in a justified manner, may extend the period of protection, after hearing the persons or bodies that may be affected.

**Independent Authority for Whistleblower Protection:** Independent administrative authority, as a public law entity at the state level, which will act in the fulfillment of its main function of protecting *Whistleblowers*. Among its other functions are the management of its own external channel, the processing of sanctioning procedures and the imposition of sanctions, among others.

**Logbook:** System through which the evidence of the information received and of the internal investigations to which they have given rise will be kept, guaranteeing, in any case, the confidentiality requirements.

#### Examples of Protections and Support Measures

*Whistleblowers* are advised of additional support measures provided for by applicable legislation. The *Independent Authority for Whistleblower Protection* may provide the following resources:

- Comprehensive information and advice on available remedies for *Harmful Conduct*.
- Effective assistance from the competent authorities.
- Legal assistance in criminal proceedings and cross-border civil proceedings.
- Financial and psychological support if deemed necessary by the *Independent Authority for Whistleblower Protection*.

## Annex V

### Measures Applicable to IRIDIUM Subsidiaries in Latin America

#### Communication Channels

In addition to the forms of *Communication* indicated in the *Communication Channels* section of this Policy, *IRIDIUM Group Members* and *Third Parties* located in Latin America may send their *Complaint* or *Inquiry* to the following addresses:

- By mail to the following address:

#### CHILE:

Canal Ético IRIDIUM Chile  
Calle José Antonio Soffia n.º 2747, Oficina 602  
Comuna de Providencia,  
Santiago, Chile

#### PERU:

Canal Ético IRIDIUM Perú  
Avenida Felipe Pardo y Aliaga 652, Oficina 304,  
San Isidro, 15073,  
Lima, Peru

- In case of *Complaints* or *Inquiries* made by *IRIDIUM Group Members*, it will also be possible to submit a written *Communication* by e-mail or a verbal *Communication* to:
  - The direct supervisor or any Director of IRIDIUM LATAM (who must inform the IRIDIUM LATAM *Compliance Committee*);
  - Any member of the LATAM *Compliance Committee*;
  - The compliance department of IRIDIUM LATAM;
  - The Crime Prevention Officer of the Crime Prevention Model of said subsidiaries.



## Annex VI

### Measures Applicable to IRIDIUM Subsidiaries in North America

#### Communication Channels

In addition to the forms of *Communication* indicated in the *Communication Channels* section of this Policy, *IRIDIUM Group Members* and *Third Parties* located in North America may send their *Complaint* or *Inquiry* to the following addresses:

- By mail to the following address:

Ethics Channel ACS Infrastructure  
One Alhambra Plaza, Suite 1200  
Coral Gables, FL 33134

- In case of *Complaints* or *Inquiries* made by *IRIDIUM Group Members*, it will also be possible to submit a written *Communication* by e-mail or a verbal *Communication* to:
  - The direct supervisor or any Director of ACS INFRA (who must inform the ACS INFRA *Compliance Committee*);
  - Any member of the ACS INFRA *Compliance Committee*;
  - The compliance department of ACS INFRA.

