



Group Whistleblowing Policy

March 2025

ISO 9001, ISO 14001, ISO/TS 29001 and
ISO 45001





Purpose & Objectives



Archirodon group of companies (the “Group”) is committed to carrying out all aspects of its business and operations in accordance with the highest professional and ethical standards and in compliance with the applicable laws and regulations.

The purpose of this Whistleblowing Policy (“Policy”) is to provide a framework for the timely detection of irregularities, omissions or criminal acts occurring during the operations of the Group.

This Policy also sets out the principles, protection measures and the general operational framework under which the Group receives, manages, and investigates reports of such irregularities, omissions or other criminal acts, which relate to the Group and are brought to the attention of its staff or third parties.

This Policy aims to:

- I. Encourage people to report attempted, suspected or actual wrongdoing as soon as possible, in the knowledge that their concerns will be taken seriously and investigated as appropriate, and in particular with confidentiality;
- II. Provide people with guidance as to how to raise those concerns;
- III. Reassure people that they should be able to raise genuine concerns in good faith, while being personally protected.



Description



1. Personal Scope

This Policy applies to former, present and candidate (where applicable):

- a. members of the Board of Directors, as well as any shareholders of the Group,
- b. all officers, employees, trainees, interns and volunteers of the Group,
- c. vendors, suppliers, contractors and anyone providing services to the Group, as well as their respective employees and sub-contractors,
- d. third parties who are aware of or suspect any irregular or illegal actions relating to the Group.

For the purposes of this Policy:

- the reporting of a Concern (as defined below) by any of the above persons is called “filing a Complaint”, and the person that reports them is called “Reporting Person or Complainant”;
- the Group includes all the subsidiaries of Archirodon Group N.V. (and notably the subsidiaries established in the European Union).



Description



2. Material Scope

We encourage filing Complaint(s), by submitting a report via the appropriate channels, as soon as possible, if a person thinks he/she has any information relating to incidents concerning the Group's activities, in the following areas (each a "Complaint" or "Report"):

A. Activities falling under EU Directive 2019/1937 and/or respective national legislation:

1. Violation of European Union law in areas designated by the EU Whistleblowing Directive, including for instance:

- Public procurement
- Financial services, products and markets
- Prevention of money laundering and terrorist financing
- Product safety and compliance
- Transport safety
- Protection of the environment
- Radiation protection and nuclear safety
- Food and feed safety, animal health and welfare
- Public health
- Consumer protection
- Protection of privacy and personal data
- Security of network and information systems



Description



2. Material Scope

2. Breaches affecting the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union ("TFEU").

3. Breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

4. Breaches of national legislation applicable only to the Group subsidiaries established in the Republic of Cyprus. Such breaches may concern:

- committing a criminal offence,
- violation of a legal obligation imposed by the laws or the regulations of the Republic of Cyprus,
- violation that endangers or is likely to endanger the safety or health of any person,
- violation that causes or is likely to cause damage to the environment.



Description



2. Material Scope

B. Violation of any other law, rule or regulations applicable to the Group:

Reports of serious irregular, unethical, illegal or criminal conduct with respect to the operational activities of the Group (other than Activities falling under EU Directive 2019/1937 and/or respective national legislation) include the following:

- An act or omission with regard to which the public interest is at stake in connection with (i) a breach or risk of a breach of a statutory regulation or of internal rules that impose a specific obligation and have been established by the Group on the basis of a statutory regulation or (ii) a risk to public health, public safety or the environment, or an improper act or omission that jeopardises the proper functioning of the public services or an undertaking.
- Questionable accounting practices, violations of internal accounting controls, financial reporting irregularities or any other auditing or financial matters (collectively, "Fraudulent Auditing and Accounting Activity")
- Fraud or deliberate error in the preparation, evaluation, review or audit of any financial statement of the Group companies
- Fraud or deliberate error in the recording and maintaining of financial records of the Group
- Public disclosures made by the Group that may not be complete or accurate
- Fraud
- Corruption/abuse of power
- Bribery, breach of gift and hospitality policy



Description



- Conflict of Interest
- Theft, embezzlement
- Forgery
- Infringement of Market Abuse Framework
- Illegal Conduct in breach of the sector specific framework applying to specific subsidiaries
- Breach of competition law
- Breach of any laws and regulations applicable to the Group
- Misuse of company resources
- Breaches of health and safety
- Human rights violation
- Discriminatory treatment of employees
- Harassment or acts of violence
- Threats, Extortion, Use of violence



Description



- Slander/libel
- Violation of the Group's Code of Ethics and Conduct, as well as any of its policies and procedures
- Any other criminal activity
- Conduct likely to damage the Group's reputation
- Breach of confidentiality
- Misconduct by any supplier
- The deliberate concealment of any of the above matters.

It is stressed out that a Report may relate to a suspicion of the above-mentioned acts and/or omissions and not necessarily to a completed conduct.

It is also highlighted that any Report not referring to the abovementioned areas, although it is important to be submitted, is not covered by this specific Policy and should be submitted through other available internal channels.



Description



3. Whistleblowing Procedure

The Whistleblowing Procedure is described in detail in CMP-WI-02 “Whistleblowing Report Receiving and Management”, which forms an integral part of this Policy.



Description



4. Protection measures when filing a Complaint

A basic and inviolable principle of the Policy is to protect the identity and confidentiality of the Reporting Person(s) and, if they are employees of the Group, to ensure their position and/or their professional development is not compromised. Therefore, the Group shall guarantee the confidentiality of the identity of persons submitting Reports and of every person allegedly involved in criminal acts or omissions.

The Group will protect the Complainants in good faith. However, it reserves the right to take action against any person or vendor involved, if it is proven that he/she intentionally or fraudulently provided false information when filing a Complaint. In any case, any person who suffers prejudice, whether directly or indirectly, as a consequence of a Report made in bad faith shall retain the protection and the remedies available to him/her under the applicable legislation.

4.1. Confidentiality

All information relating to a Complaint will be treated confidentially and special technical and organizational measures (i.e., pseudonymization) will be implemented.

Such information and/or the Reporting Person's identity will not be disclosed (directly or indirectly) to any unauthorized person/entity, unless the Reporting Person has provided his/her consent for disclosure.

The obligation of confidentiality is also vested upon any person(s) accused of committing the reported conduct ("Reported Person(s)"), as well as any person being named in the Complaint.



Description



4. Protection measures when filing a Complaint

By way of derogation, any information relating to a Complaint, including the Reporting Person's identity, may be exceptionally disclosed without the Reporting Person's consent upon his/her proper, written notification in the following cases:

- a. when this is required under national and/or European legislation,
- b. in the context of an investigation by the authorities, or
- c. in the context of judicial proceedings,

and only when this is necessary for handling the Complaint or to secure the defending rights of the Reported Person as per applicable legal provisions(s).

The identity of the Reported Person is respectively protected during the follow-up on the Complaint.

4.2. Eponymous and anonymous reports

Through the established channel of communication, the Group enables Reporting Persons to submit their Complaint either eponymously or anonymously.

However, the Group encourages Reporting Persons to submit their Report by name, as it creates a better communication channel for both the provision of further clarifications and the follow-up on the Complaint.



Description



4. Protection measures when filing a Complaint

4.3. Public disclosures

The Group will protect the Reporting Person who makes a public disclosure if any of the following conditions is fulfilled:

- a) the Reporting Person first reported internally and externally, or directly externally, but no appropriate action was taken in response to its Complaint within the period of three (3) months from the acknowledgment of receipt, or if no acknowledgment has been sent to the Reporting Person, three (3) months from the end of seven (7) working days from the submission of the Complaint.
- b) the Reporting Person has reasonable grounds to believe that: (i) the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or (ii) in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach. This protection does not cover the persons who have any relationship with the subsidiaries companies established in the Republic of Cyprus and directly disclose information to the press pursuant to specific national provisions establishing a system of protection relating to freedom of expression and information.



Description



4. Protection measures when filing a Complaint

4.4. No retaliation

The Group is committed to the protection of the Reporting Person(s), if they have submitted the report in good faith and they have reasonable ground(s) to believe that their Complaint is true and falls into the subject-matter scope of the Policy.

The same protection shall also be afforded to any intermediaries or third parties (natural or legal persons) that are linked to the Reporting Person or their Complaint.

The Group will not tolerate any form of retaliation, nor threats or attempts thereof, in view of the Complaint, including:

- a. suspension, lay-off, dismissal or equivalent measures
- b. demotion or withholding of promotion
- c. transfer of duties, change of location of place of work, reduction in wages, change in working hours
- d. withholding of training
- e. a negative performance assessment or employment reference
- f. imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty



Description



4. Protection measures when filing a Complaint

- g. coercion, intimidation, harassment or ostracism
- h. discrimination, disadvantageous or unfair treatment
- i. failure to convert a temporary employment contract into a permanent
- j. failure to renew, or early termination of, a temporary employment contract
- k. intentional harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income
- l. blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry
- m. early termination or cancellation of a contract for goods or services
- n. cancellation of a license or permit
- o. psychiatric or medical referrals
- p. refusal to or deprivation of reasonable adjustments to disabled persons.



Description



4. Protection measures when filing a Complaint

Any such form of retaliation is considered a serious breach of the Policy and must be immediately reported to the Compliance Committee.

Any employee or officer, regardless of position or title, who has been determined to have engaged in retaliatory measures in violation of this Policy, will be subject to appropriate disciplinary action, up to and including the termination of his/her employment or any other working relationship with the Group.

In cases when the Reporting Person suffers from damage and/or detriment, it shall be presumed that the damage and/or detriment was made in retaliation for the report or the public disclosure. In such cases, it shall be for the reported person or the person who has taken the detrimental measure to prove that that measure was based on duly justified grounds. The Group acknowledges that the Reporting Person has access to appropriate remedial measures and the right to be protected from any form of retaliation.

4.5. Personal Data

The processing of personal data included in the Complaints and respective follow- up/investigation proceedings, is carried out in accordance with national and European legislation regarding personal data protection and with the relevant policies and privacy notices of the Group, in particular the Privacy Statement for Archirodon Whistleblowing Channel as annexed to the CMP-WI-02 "Whistleblowing Report Receiving and Management".



Description



5. Whistleblowing Process & RAMR

The Whistleblowing Officer plays a central role in the proper implementation of this Policy. The Whistleblower Officer is the Responsible Person for the Acceptance and Monitoring of Reporting (“RAMR”).

For the purpose of submitting such reports, Reporting Persons are entitled to use the Group’s whistleblowing channel accessible at <https://www.archirodon.net/about-us/ethics-compliance/>, always maintaining the confidentiality of the Reporting Persons’ identity and the reported incidents.

Reporting Persons are thus encouraged to report any irregularities using the aforementioned whistleblowing channel (“internal reporting”) rather than approaching competent authorities (“external reporting”).

Reporting the irregularities using this whistleblowing channel will however not prejudice the right of the Reporting Persons, to file a Complaint directly with a regulatory authority or any other relevant government body where they believe that this is the only appropriate course of action.

Anyhow, the Whistleblowing Officer shall provide assistance and access to any competent public, administrative or judicial authority, during the investigation of such incident or conduct, if requested by them and according to the applicable legislation.



Description



6. Role and responsibilities of the Whistleblowing Officer (internal reporting)

The Whistleblowing Officer shall provenly possess a high level of personal and professional integrity, as well as impartiality, objectivity, confidentiality and shall be involved in all steps of the process, ensuring that the Policy is implemented.

The Whistleblowing Officer is responsible for handling the Reports, including the receipt, registration, **processing** and monitoring of the Complaints falling within the scope of this Policy.



Description



7. Complaints submitted directly to the competent authorities of each member state of EU (external reporting)

As stated above, the Reporting Persons have the right to file a Complaint through external reporting channels towards any competent regulatory authority of each member state of EU, that has the power to receive, manage and monitor complaints under EU Directive 2019/1937 or to any other competent authority depending on the subject of the Complaint.

The external report shall be submitted in writing or orally – via telephone or other systems of oral messaging, and via a personal meeting – via email or via an electronic platform, accessible to persons with disabilities.

The Reporting Persons are encouraged to report the Complaint internally (within the Group) first, where the breach can be addressed effectively and where they consider that there is no risk of retaliation.

In any case, Reporting Persons are free to choose whether to report the Complaint first internally or to report it directly externally to the competent authorities.

It is noted that in case the Reporting Person submits his/her Report both internally and externally, the procedures initiated upon the internal Report are terminated.



Description



8. Penalties

Employees of the Group, who:

- a. hinder or attempt to hinder the submission of a report to the internal or external reporting channels,
- b. retaliate or initiate malicious proceedings against the Reporting Persons,
- c. breach the duty of maintaining the confidentiality of the identity of Reporting Persons,

may be punished with criminal sanctions and monetary fines pursuant to the applicable legislation.

Employees who proceed in knowingly false reporting or public disclosures shall face equivalent sanctions, including penalty of imprisonment and monetary fines.

Reports are considered to be made in bad faith, if they are made maliciously, with reckless disregard for their truth or falsity and/or for the sole purpose of harming the Group and/or the Reported Person(s) or any other persons.

Employees making such a report in bad faith may be subject to disciplinary measures or other employment actions at the discretion of the Group.



Responsibility for Implementation



The Whistleblowing Officer is responsible for handling the receipt, registration, processing and monitoring of the Complaints falling within the scope of this Policy.

The Compliance Officer carries out the initial evaluation of the Complaint (Category A, B or C).

Depending on the category of the Complaint, the Compliance Officer and/or the HR Director are responsible for the investigation of the Complaints.

The Compliance Committee is responsible for overall assessing and handling of the investigation reports and proposing measures it deems necessary.

The Competent Body/Officer designated by the Compliance Committee in accordance with the circumstances of the case (such as the Chief Executive Officer, the board of directors of the company to which the Complaint is addressed, the Project Director, etc., depending on the nature of the incident and of the persons involved), takes appropriate measures to address the incident.

The Compliance Officer is responsible for updating this Policy in order to recognize changes of the respective regulatory framework and continually improve its efficiency and effectiveness.

In addition, the Compliance Officer must ensure that employees throughout Archirodon Group have understood their rights, obligations and responsibilities pursuant to this Policy.



Whistleblowing Report Receiving and Management

ISO 9001, ISO 14001, ISO/TS 29001 and
ISO 45001





ROLE AND RESPONSIBILITIES OF THE WHISTLEBLOWING OFFICER



The Whistleblowing Officer is responsible for handling the Reports, including the receipt, registration and monitoring of the Complaints falling within the scope of this Policy.

In particular, the Whistleblowing Officer shall undertake the following duties:

- providing necessary information regarding the possibility of submitting a Complaint within the Group and disclosure of such information in a visible spot,
- receipt of the Complaints,
- confirming Complaint's receipt to the Reporting Person within seven (7) working days from the day of submission,
- taking actions so that the Compliance Officer addresses the Complaint or terminates the procedure and archives the Complaint if it: a) is unintelligible or b) is submitted abusively or c) does not substantiate a breach or does not include major indications for such a breach or d) is out of scope of the Whistleblowing Policy. The decision for archiving the report is notified to the Reporting Person, who may resubmit the report to the competent national authority ("external reporting"),
- ensuring the protection of confidentiality of the Reporting Person's identity, as well as of any third person named in the report,



ROLE AND RESPONSIBILITIES OF THE WHISTLEBLOWING OFFICER



- monitoring the Complaints and maintaining communication with the Reporting Person,
- informing the Reporting Person regarding the actions that have been taken within a reasonable term, not exceeding three (3) months from the confirmation of receipt,
- providing clear and accessible information for the procedures of submitting Complaints to the competent national authority and to entities of the public sector or other institutions or organizations of the European Union,
- designing and coordinating training sessions regarding ethics and integrity,
- participating in the development of internal policies to enhance integrity and transparency in the Group.



RECEIPT OF COMPLAINT



The Group in order to encourage the filing of Complaints has created a special communication channel that may be used by the Reporting Persons.

Each Complaint filed should include: the main cause of the Complaint (acts that may potentially cause or have caused a reportable incident), with specific information (e.g. names, dates, location) and if possible substantiation through relevant documents or other records.

It is not necessary to include evidence inside the Complaint submission, but any relevant information that will facilitate the assessment of the Complaint will be considered.

Complaints shall be submitted via the Whistleblowing channel, which can be accessed via the following URL
<https://report.whistleb.com/en/archirodon>

The above Whistleblowing channel operates as communication channel for reporting and is available all days and hours during the week.

Complaints may also be sent directly to the Whistleblowing Officer to the email address: whistleblowing@archirodon.net and compliance-officer@archirodon.net.

Any expression of complaint, dissatisfaction, opinion and/or grievance, which is not submitted through the present Whistleblowing Procedure may not be treated as a Complaint by the Group.

It is noted that a Report filed via the Whistleblowing channel will be handled at Group level, whilst the measures to remediate the incident reported will be taken by the competent body/officer designated by the Compliance Committee in accordance with the circumstances of the case (such as the Group's Chief Executive Officer, the board of directors of the company to which the Complaint is addressed, etc., depending notably on the nature of the incident and of the persons involved)) ("Competent Body/Officer").



RECEIPT OF COMPLAINT



A designated member of the Legal and Contracts Department of the Group operates as the Whistleblowing Officer for all Group's companies, unless otherwise required under applicable legislation, and is responsible for receiving reports and informing the Compliance Officer with respect to the Complaints.

In case the Complaint is submitted through the Whistleblowing channel, the latter notifies the Reporting Person of the receipt within seven (7) days. If the Complaint relates to the Whistleblowing Officer, he/she must be replaced in handling the specific Complaint by the Data Protection Officer who will act as a Deputy Whistleblowing Officer.

The Compliance Committee consists of the Group's (i) two Chief Operation Officers, (ii) Chief Financial Officer (iii) Compliance Officer and (iv) Central Functions Director, supported by any other extra job position, if needed, as the case may be. The Compliance Committee monitors, guides and evaluates the incident reports provided by the Compliance Officer (as the case may be) and monitors the overall effectiveness of applicable compliance practices, as reported by the Compliance Officer.

If the Complaint relates to any of the members of the Compliance Committee this member must abstain from the process. In the event of conflict of interest, the member of the Compliance Committee subject to the conflict should abstain from the procedure.

The Compliance Officer, in the exercise of his/her duties related to the Whistleblowing Policy and the present procedure is supported by the Compliance team.



HANDLING OF COMPLAINT



The Compliance Officer of the Group, supported by the Compliance team, shall inform the Compliance Committee within a reasonable period of time, the latest within one (1) month following receipt of the Complaint, conducting an initial assessment and examining the key elements of the Complaint.

In any case, deadlines set by the applicable legal framework, including the relevant framework for the processing of personal data, shall be respected, with emphasis on the obligation to notify the Reporting Person about the status of his/her Complaint within three (3) months after its submission.

It is expressly stated that the Group shall share resources as regards the receipt of reports and any investigation to be carried out, by using the internal reporting channel accessible to all the subsidiaries companies.

The Group guarantees that persons acting as Whistleblowing Officer or participating in the Compliance Committee are bound by enhanced confidentiality clauses and may transfer any information they receive in the course of their duties when investigating a Complaint solely to the Group company to which the Complaint is addressed.



EVALUATION OF COMPLAINT



Subsequently, the Compliance Officer shall carry out an initial assessment on the core of the Complaint, examining the credibility and validity thereof, in order to categorize it accordingly, into the following categories A, B or C, and shall promptly inform the Group's Compliance Committee for the cases received and their categorization to the below categories.

Category A: Vague/unfounded Complaint

Where the Complaint is out of scope, not sufficiently justified or is clearly unfounded due to unreliable information, the Compliance Officer will decide that no further investigation is required and shall subsequently inform the Whistleblowing Officer.

Category B: Labor/interpersonal relations

If the Complaint relates to labor or interpersonal relations within the Group (e.g. harassment, use of force/violence, unethical workplace behavior, insult, etc.), the handling of the Complaint and its further investigation is handled in consultation with, or assignment to the HR Director, unless provided otherwise by the applicable local legislation or by a specific Group or local policy. Upon conclusion of the investigation, the findings of the investigation are handled by the Compliance Officer, for further actions, in consultation with the Compliance Committee.

Category C: Other Issues

If the Complaint concerns actions or omissions described in this Policy (other than the ones belonging to Category B), then the handling of the Complaint and its further investigation is assigned to the Compliance Officer, in consultation with the Compliance Committee.



SELECTION OF INTERNAL INVESTIGATION METHODS



With regard to a Complaint falling under Categories B and C above, the Compliance Officer and/or the HR Director (as the case may be), after consulting with the Compliance Committee, if required, shall take the following actions:

- 1) Determine the scope and type of the investigation to be carried out. Indicatively and in accordance with applicable policies:
 - i. interviews may be conducted to gather evidence and/or assess its probative value;
 - ii. an autopsy and/or on-site inspection may be carried out at the company's premises/project's site, as required;
 - iii. special consultants may be engaged (experts, psychologists, economists, legal advisors, IT companies, etc.);
 - iv. an audit on the company's IT resources may be carried out.
- 2) Ensure that the evidence gathered through the investigation is used in such a way to safeguard the lawfulness of the process and the rights of the parties involved.
- 3) Take all the appropriate measures for the conduct of the investigation regarding the Complaint received.



REPORTING



Upon completion of the investigation, the Compliance Officer prepares the investigation report with the investigation's findings and sends it to the Compliance Committee.



RESOLUTION AND REMEDIATION



Following the receipt of recommendations as included in the investigation report, the Competent Body/Officer implements measures to address and remediate the incident, if feasible and informs the Compliance Officer and the Whistleblowing Officer of the actions taken, for the latter to inform the Reporting Person accordingly.

Furthermore, the Competent Body/Officer and/or the Compliance Officer, in collaboration with the Compliance Committee, if required, shall examine the obligation to notify the Reported Person(s) or other parties involved, such as other companies of the Group involved and potentially the supervisory authorities.

If the Competent Body/Officer and/or the Compliance Officer wish to take judicial action against the parties involved to defend the Group's legitimate interests, the Compliance Officer, in consultation with the Compliance Committee, shall be instructed to initiate such procedure. If the case takes the judicial route, the Compliance Officer along with the Compliance Committee shall monitor the progress of the case.

Finally, the Competent Body/Officer and/or the Compliance Officer shall take appropriate measures to ensure, if possible, that the cause of the Complaint is eliminated.



MONITORING AND FUTURE IMPROVEMENT



The Competent Body/Officer and/or the Compliance Committee shall make recommendations for improving and optimizing current policies and procedures for the avoidance of similar incidents in the future.



STEPS DESCRIPTION



A/N	Responsible Party	Activity / Action Description
1	Reporting person	Submit a Complaint Submit a report of an irregularity, omission, or criminal act through Archirodon's whistleblowing channel (https://www.archirodon.net/about-us/ethics-compliance/) or through email.
2	Whistleblowing Officer / Compliance Officer	Stage One: Receipt of the Complaint by the Whistleblowing Officer The Whistleblowing Officer notifies the Compliance Officer on the receipt of a report and confirms the receipt of the Complaint to the Reporting Person within seven (7) days.
3	Whistleblowing Compliance Officer/ Compliance Committee	Stage Two: Evaluation of the Complaint The Compliance Officer of the Group conducts an initial assessment, examining the credibility and validity of the Complaint, in order to categorize it into categories A, B or C (as described below), as appropriate, reviewing also the key elements of the Complaint in order to clarify to which company of the Group it relates.
4	Compliance Officer	Category A: Vague Complaint Where the Complaint is out of scope, not sufficiently justified or is clearly unfounded due to unreliable information, the Compliance Officer will decide that no further investigation is required. In such case, the Complaint is archived and the Reporting Person is informed of this outcome by the Whistleblowing Officer within three (3) months from the filing of the Complaint. Completion of the Process.



STEPS DESCRIPTION



A/N	Responsible Party	Activity / Action Description
5	Compliance Officer/HR Director	Category B: Labor & Interpersonal Relations Matters In case the Complaint concerns labor or interpersonal relations matters within the Company (e.g., harassment, use of violence, unethical behavior in the workplace, insult, etc.), the handling of the Complaint and its further investigation is handled in consultation with, or assignment to the HR Director, (unless provided otherwise by the applicable local legislation or by a specific Group or local policy). Upon conclusion of the investigation, the findings of the investigation are handled by the Compliance Officer, for further actions, in consultation with the Compliance Committee.
6	Compliance Officer, Compliance Committee	Category C: Other Issues In case the Complaint relates to actions (other than Category A and B) described in this Policy, then the handling of the Complaint and its further investigation is entrusted to the Compliance Officer, in consultation with the Compliance Committee.
7	Compliance Officer	Stage Three: Information of the Compliance Committee The Compliance Officer informs the Compliance Committee about the categorization of the Complaint to Categories B and C, according to Stage 2.
8	HR Director/ Compliance Officer	Stage Four: Selection of Internal Investigation Methods The Compliance Officer and/or the HR Director (as the case may be), after consulting with the Committee, if required, shall take the following actions: <ul style="list-style-type: none">-Review of the necessity to involve external partners for resolution (if necessary, contact an external partner).-Selection of appropriate investigative measures (e.g. interviews with the parties involved, collection of evidence, etc.).



STEPS DESCRIPTION



A/N	Responsible Party	Activity / Action Description
9	HR Director/ Compliance Officer/Compliance Committee	Stage Five: Reporting Upon completion of the investigation, the Compliance Officer prepares the investigation report with the investigation's findings and sends it to the Compliance Committee.
10	Competent Body/Officer/Compliance Committee/Whistleblowing Officer	Stage Six: Resolution and Remediation The Competent Body/Officer shall: -implement appropriate measures and inform the Compliance Officer and the Whistleblowing Officer of the actions taken, for the latter to inform the Reporting Person accordingly. -explore further legal actions, if necessary, against the parties involved, in which case the Compliance Committee shall be instructed to initiate such procedure. If the case takes the judicial route, the Compliance Officer along with the Compliance Committee shall monitor the progress of the case. -in collaboration with the Compliance Committee, if required, shall examine the obligation to notify the Reported Person(s) or other parties involved and the relevant national supervisory authority, if necessary.
11	Compliance Committee/ Competent Body/Officer	Stage Seven: Monitoring and Future Improvement The Competent Body/Officer and/or the Compliance Committee shall make recommendations for improving and optimizing current policies and procedures for the avoidance of similar incidents in the future.



Appendix



Privacy Statement for Archirodon Whistleblowing Channel

The processing of all personal data included in the Complaints (as defined in CMP-POL-03 “Group Whistleblowing Policy”) and respective follow-up/investigation proceedings, is carried out in accordance with national and European legislation regarding personal data protection. In particular:

Why does the Archirodon group of companies (the “Group”) process personal data? The personal data of all parties involved in the Complaint are protected and processed solely in the context of prevention, detection or investigation of irregular, unethical, illegal or criminal behavior.

Is the Group legitimized to process personal data? For alleged offences against public interest or related to incidents of violence and harassment in the workplace, processing is a legal obligation of the Group. For other alleged offences, it is in the legitimate interests of the Group or third parties to proceed with the processing of information relating to illegal or irregular conduct, that exposes the Group to financial, legal and reputational risks, or damage its corporate culture and cause a negative working environment.

Who can access the personal data of the person(s) involved? Only those involved in the management and the investigation of the Complaint can access the data contained in the reports, if necessary. In particular, the recipients of personal data included in Complaints may be the Whistleblowing Officer, the members of the Group's Whistleblowing Committee (as described in CMP-WI-02 “Whistleblowing Report Receiving and Management”), external consultants bound by confidentiality clauses, lawyers, the provider of the online reporting platform (if any), as well as judicial and/or administrative authorities.



Appendix



Privacy Statement for Archirodon Whistleblowing Channel

How long will the Group retain the personal data of the person(s) involved? The Group will retain personal data for a certain period of time upon the completion of the investigation, which varies depending on the outcome of the investigation.

In particular:

- If the report is deemed unfounded, the personal data shall be deleted within two (2) months from the date of its filing.
- If the reported situation follows the judicial recourse, the personal data shall be erased upon issuance of the respective final court decision.
- If the report results in substantiated findings against an employee, officer or executive of the Group, the personal data shall be retained for the duration of his/her employment/relationship with the Group and shall be deleted twenty (20) years after the termination of the cooperation.
- If the report results in substantiated findings against an external partner, vendor, contractor or supplier of the Group, the personal data shall be retained for the entire duration of his/her cooperation and shall be deleted five (5) years after the termination of such cooperation.

Is the personal data of the person(s) involved safe? The Group implements the necessary technical and organizational measures to ensure a high-level data security (such as access to information "on a need-to-know basis", imposing confidentiality obligations to the personnel who has access with a, recording accesses, monitoring accesses and access rights, use of encryption, keeping passwords confidential, etc.).

Informing Reported Persons: Reported Persons and any other persons named in the Complaint, shall not be informed on the processing of their personal data as normally required under applicable data protection legislation, for as long as necessary, in order to prevent and confront any attempts to obstruct the handling of the Complaint or the taking of non-retaliation measures. Accordingly, any data subject requests exercised by any Reported Persons or relevant named persons, may not be satisfied. In case of doubt, the Data Protection Officer must be consulted ad hoc.