ALERT REPORTING & INVESTIGATION PROCEDURE

GENERAL REQUIREMENTS

PURPOSE

- Pharming Group N.V. and all of its affiliates and entities worldwide (collectively, “Pharming”) are committed to doing business with integrity and complying with applicable legal and ethical standards, categorically rejecting fraud, corruption, harassment, discrimination and any other form of misconduct.
- Pharming strongly believes in an open culture where all individuals are encouraged at any moment to speak up and report their concerns.
- In accordance with its Code of Conduct, Pharming has implemented this alert reporting and investigation procedure (the “Procedure”) allowing employees, contractors, and any other individuals working for or hired by Pharming ("Pharming Personnel") to report alerts on conduct that does not comply with Pharming’s Code of Conduct, policies, procedures, ethical principles or legal obligations, as defined below.
- As a result, the purpose of this Procedure is to define the principles and requirements relating to Pharming's alert reporting and investigation process (the “Alert Reporting Process”) primarily for use by the functions involved in alert-reporting and investigations.
- This Procedure implements laws, regulations and codes related to alert reporting (e.g., EU Directive 2019/1937 and the Dutch Whistleblowers Protection Act).
- The Procedure will also be activated in case of in-scope incidents by Pharming Personnel and/or members of the Board of Directors, that has been detected by Business Integrity or any other control function in the exercise of their activities (e.g., monitoring, advisory work, meeting participation, document review, audit findings or any other source).

SCOPE

- This Procedure applies to Pharming Personnel globally.
- Alerts must be managed in compliance with applicable laws in the country in which the Pharming Personnel live or perform their professional activities for Pharming.
- In the event of any conflict between this Procedure and laws, regulations, codes, or other applicable Pharming policies and procedures, the more restrictive requirement will apply.
- Any exception to this Procedure must be approved in writing by Business Integrity.

MATTERS TO REPORT

- Pharming Personnel must promptly report actual or suspected incidents of a serious operational or financial nature within operations related to Pharming, including – as examples - the imminent or actual:
  - performance of criminal acts, such as fraud, anticompetitive behavior, bribery or corruption;
  - discrimination, harassment, intimidation, and other infractions of employees’ rights;
  - endangerment of patients’ health, public health, safety or the environment or any conduct where public interest is at risk;
  - violation of Pharming’s policies and procedures that potentially expose Pharming to the above risks;
  - suppression, destruction, withholding or manipulation of information on the incident concerned;
  - violation of ethical or professional standards, including the standards set out in the Code of Conduct;
  - violation of applicable laws, regulations and codes.
- Alerts must be reported on facts and made in good faith.

NO-RETALIATION

- Pharming is committed to a strict non-retaliation policy and will not discharge, demote, suspend, threaten, harass, bully, intimidate or in any manner retaliate against any individual for reporting an alert in good faith, even if the reported actions later turn out to be inaccurate. This includes any retaliation against people and third parties who assist the person making the report (e.g., a family member, a lawyer, a confidential advisor or trade union representative). It also includes those involved in managing and conducting the investigations (e.g., Business Integrity, Legal, Internal Controls).
- Disciplinary proceedings may be taken against the instigators of any such retaliatory behaviour.
- Abuse of the Alert Reporting Process is prohibited. Malicious reports, or alerts reported in any other manner which is not truthful and in good faith, will be investigated under normal investigation and disciplinary actions may apply.

CONFIDENTIALITY & ANONYMITY

- To the extent reasonably possible in the conduct of an investigation, matters reported will be handled confidentially at all stages of this process by all those involved and in accordance with the applicable laws, regulations and codes. This applies to the personal data of individuals that report an alert, as well as to those of the individuals subject to an alert.
- Pharming Personnel can make anonymous reports, but they are encouraged to identify themselves in case more information is needed during the investigation. Confidentiality will be maintained to the extent possible in light of the need to fully investigate the reported concerns.
  - Where required by law, the identity of the person who raised a report and the information that can be used to directly or indirectly determine the identity of the person who raised a report shall not be disclosed without the consent of this person. Should disclosure of the identity of the person who raised a report occur, as referred to above, a person who raised a report or a person concerned shall receive an explanation in writing containing the reasons for the disclosure of the information regarding their identity.
- The identity of the person subject to an alert must be kept confidential, unless
  - disclosure is required by the authorities based on legal requirements (in which case, the reporting personnel shall be notified in advance of such disclosure, unless such information would jeopardize the related investigation or legal proceedings); or
  - needed to fully investigate the reported concerns.
- Alerts will be processed by Business Integrity and other Pharming Personnel designated by Business Integrity, including (without limitation) relevant members of Business Integrity, Legal, HR or other control functions in the US in case of alerts relating to US Pharming Personnel. For that purpose, Business Integrity will set-up an investigation team for the relevant alert, including the aforesaid members as applicable. All other Pharming Personnel are explicitly prohibited from personally investigating alerts or any potential misconduct or violation.
- Only Business Integrity and the designated Pharming Personnel in charge of the treatment of an alert have access to the related information. Information is transmitted on a strict need-to-know basis.
- All persons involved in the treatment of alerts are bound to an obligation of confidentiality.
- Any persons involved in the investigation process must remain impartial and ensure no actual, potential or perceived conflict of interest exists.
- Information of a confidential nature that needs to be protected as outlined above includes:
  - information about the identity of the reporter and of the person to whom the alert is attributed or with whom that person is associated and information that can be traced back to this.
  - information about a trade secret.

DATA PROTECTION

- Personal data can be collected only if it is relevant, adequate and limited to what is necessary in line with the applicable laws, regulations and codes.
- The use of personal data collected in this process is strictly limited to the treatment and investigation of alerts.
- The following categories of personal data can be collected by the recipient of the alert:
  - Identity of the person who raised the alert: name, position and professional contact details;
  - Identity of the person subject to an alert: name, position and professional contact details;
  - Identity of the person(s) who will treat the alerts(s): name, position and professional contact details;
  - Details of facts reported and all aspects of the matter being investigated, which may include health data of the person who raises the alert, the identity of the person subject to an alert, or other data needed to meet adverse event reporting requirements.
- Access to data related to alerts is restricted to Business Integrity and the designated employees.
- Employees whose personal data is treated within the Alert Reporting & Investigation Procedure process have the right to query, access, rectify, erasure, portability of their own personal data, as well as the right to object and restrict the processing of the data for legitimate cause. These requests must be sent to the following address: gdprcompliance@pharming.com. However, the person subject to an alert can under no circumstances obtain information concerning the identity of the person reporting the alert based on their data access right.

DATA RETENTION

- Data related to alerts is not retained for a longer period than necessary for the investigation and related actions and reporting. Alerts can be diverse in nature size. In any case, if the individual making the alert is reachable, Pharming will confirm receipt of the alert within 7 days of receipt thereof and provide feedback - on the status/progress of the investigation - to the person that raised the alert within 3 months from the date of the receipt notice.
- In case of a litigation process, archived data is stored in an information system with limited access and for no longer than the end of the period applicable to the litigation process.
- Data related to alerts will be archived wherever possible in an anonymized fashion and in a confidential and secure way for a period not exceeding 5 years.
- Personal data can be transferred to entities of Pharming or third parties registered in countries outside of the European Economic Area if Pharming ensures that these transfers comply with local data protection laws and implements adequate protection guarantees, such as the adoption of contractual standard clauses established by the European Union.

INDIVIDUALS RAISING ALERTS

- Alerts can be raised by:
  - Pharming Personnel generally.
  - Business integrity or any other control function in the exercise of their activities (e.g., monitoring, advisory work, meeting participation, document review, audit findings or any other source).
  - Other individuals (e.g., job applicants, contractors, shareholders, and suppliers, interns, trainees, former employees or employee's relatives).
- Raising an alert cannot provide any advantage to the individual raising it. They must not be compensated for raising an alert.

An individual raising an alert has the right, and shall be given the opportunity by Pharming, to consult with an independent confidential counsellor concerning the alert. Such counsellor shall be designated by Business Integrity.

PROCESS STEPS

1. HOW TO RAISE AN ALERT

- Individuals wanting to raise an alert are encouraged to reach out, orally, in writing or electronically, to:
  - their manager (unless this person is involved in the subject of the alert);
  - Human Resources;
  - Business Integrity; or
  - Any other internal or external channel available to them based on local laws, regulations and codes.
- Individuals wanting to raise an alert concerning the functioning of:
  - a person working in Human Resources or Business Integrity, may report directly to any member of the Executive Committee of Pharming Group N.V.;
  - a member of the Executive Committee, other than the CEO, may report directly to the CEO;
  - the CEO, may report directly to any member of the board of directors of Pharming Group N.V. (the "Board of Directors");
  - a member of the Board of Directors who is not the chairperson of the Board of Directors, may report to the chairperson of the Board of Directors; and
  - the chairperson of the Board of Directors, may report to the CEO or the Vice-Chair of the Board of Directors.
- Individuals wanting to raise an alert may also contact the Pharming Helpline as follows:
  - Phone: +31(0)71 524 710 Europe and International/ +1 (844) 701-6378 in the United States only
  - Email: alert@pharming.com
  - Postal address: attn. Business Integrity Department, Vondellaan 47, 2332 AA Leiden, The Netherlands.
- Alerts can be raised in any language.

2. RECEIPT OF ALERTS

- All alerts – both if reported by individual Pharming Personnel members and if detected by control functions in the exercise of their activities - are received and recorded by Business Integrity in an alert registry or equivalent system. Business Integrity will report each alert without undue delay to the Chief Ethics & Compliance Officer.
- Where required by law, if a report is made by telephone or other voice message system, Pharming must register this report. It can do this by:
  - recording the conversation and save it as such (the reporter must give consent in advance);
  - by storing an accurate written record (transcription) of the conversation.
  - If a written record is stored, the reporter must be given the opportunity to check the written record, correct it if necessary and approve it.
- Business Integrity (or individuals designated by them) are only allowed to communicate with the person raising the alert.
- Within 7 days from the receipt of the alert, wherever technically possible, Business Integrity confirms receipt thereof to the individual who raised the alert (receipt notice). This receipt notice does not imply that the alert is admissible.
- Following receipt, each alert is subject to a preliminary evaluation by Business Integrity, with a view to determine whether the alert is within the scope of the Alert Reporting & Investigations Procedure and whether it requires further investigation or whether it is unfounded or to be considered as a minor breach or unplanned deviation. In case Business Integrity is the subject of the alert or there is any potential conflict of interest, another function can be assigned by Business Integrity to perform this preliminary evaluation (e.g., Internal Control or Human Resource).
- Once this determination has been made, Business Integrity will arrange to discuss the matter with the person raising the alert. This discussion serves the purpose of requesting further documentation or ask questions.
- The person raising the alert must be informed that it will not always be possible to share the outcome of an investigation. However, they should be informed that the matter is being looked into and that they will be notified when it is concluded.
- In any case, Pharming will provide feedback - on the status/progress of the investigation - to the person that raised the alert within 3 months from the date of the receipt notice.

3. CONDUCT OF INVESTIGATIONS

- Any alert – both if reported by individual Pharming Personnel members and if detected by control functions in the exercise of their activities - deemed admissible and in scope of the Alert Reporting Process will trigger an investigation based upon a preliminary determination made by Business Integrity. Business Integrity will report the start of each investigation without undue delay to the Chief Ethics & Compliance Officer.
- Business Integrity is responsible to define the investigation strategy (e.g., interviews, written statements, surveillance, document review), document and retain evidence gathered.
- Wherever possible, the allegations are conveyed to the individual accused, who is given the opportunity to respond and defend themselves against the allegations.
- Business integrity must have full access to all records/documents/information as they may deem appropriate, in line with applicable laws. No one within Pharming can directly or indirectly, expressly or implicitly cause an obstacle to the investigation process or attempt to influence the individuals conducting the investigation.
- All evidence obtained should be recorded chronologically in a log or inventory. Examples of evidence include the following:
  - Letters, memos, and correspondence (in hard copy or electronic form);
  - Financial records;
  - IT or systems access records;
  - Phone records;
  - Customer or vendor information (e.g., contracts, invoices, and payment information);
  - Public records (e.g., property records or business registrations filed with government agencies);
  - News articles;
  - Websites (e.g., social networking sites),
- Depending on the subject matter and the circumstances of the alert, Business Integrity may involve other functions into the investigation team, such as, but not limited to Legal, Human Resources, Quality, Finance, Medical and these can be associated to the investigation team and process. For alerts involving alleged fraud Legal and Internal Control must be part of the investigation team. A strict duty of confidentiality is requested under such collaboration.
- If deemed necessary, external counsel, or forensic experts may be enrolled into the internal investigation by Business Integrity only.
- All employees, including all levels of management, must cooperate fully with and provide appropriate assistance to ongoing investigations, and must maintain the confidentiality of investigations.
- Investigations will be conducted as expeditiously as possible, without jeopardizing the integrity of the investigation.

4. OUTCOME OF THE INVESTIGATIONS

- At the outcome of an investigation, an investigation report is generated by Business Integrity. Such investigation report may contain observations, conclusions, resolutions, and disciplinary actions or corrective actions.
- Business Integrity assesses the severity of any infraction, performs root-cause analysis, and recommends preventative measures where applicable
- For any incident of significant fraud or corruption, a draft of the proposed final investigation report should be submitted to external legal counsel as engaged by the investigation team for review. To be covered by the attorney-client privilege, the report must be addressed to counsel. If previously issued financial statements for one or more years may have been adversely affected, the Executive Committee and the Corporate Governance Committee should be notified.
- If the investigation report requires disciplinary actions:
  - Business Integrity, Human Resources and management of the function involved will determine whether disciplinary action will be taken and, if so, whether the appropriate disciplinary action in is line with the seriousness of the violation and the applicable employment laws, regulations, and codes. Examples of disciplinary actions may include:
    - Managing performance (e.g., coaching, training);
    - Verbal warning (documented and placed in employee's Human Resources personnel file);
    - Written warning (acknowledged by employee and placed in employee's Human Resources personnel file);
    - Disciplinary sanction (e.g., change in role, job level, or salary plan, reduction up to possible cancellation of the bonus);
    - Requesting voluntary financial restitution;
    - Reporting the incident to law enforcement or regulatory bodies, encouraging them to prosecute, and cooperating with them;
    - Filing a civil suit to recover the amount taken;
    - Filing an insurance claim;
    - Reporting to the perpetrator's professional association;
    - Dismissal and termination of contracts including with third-parties;
    - Legal action (e.g., civil or criminal).
  - Business Integrity, Human Resources and management of the function involved may determine that suspension is needed even prior to the conclusion of an investigation.
  - Business Integrity and Human Resources will involve the management of the function involved, as advisors only, in determining any potential disciplinary action.
  - If the individual under investigation is a member of the Executive Committee, then the CEO and the Chairman of the Board will be consulted by the Chief Ethics and Compliance Officer. If the individual under investigation is a member of the Board, then the Chairman of the Board will be consulted by the Chief Ethics and Compliance Officer. If the individual under investigation is the Chair of the Board, then the Vice-Chair of the Board will be consulted by the Chief Ethics and Compliance Officer. The Chief Ethics and Compliance Officer is responsible to keep the Board updated on the evolution of the case in a manner which does not impact the appropriate roll out and independence of the investigation. If the individual related to the alert is the Chief Ethics and Compliance Officer, then the above role is performed by the CEO.

- Human Resources is responsible for implementing the disciplinary action for staff members and confirming to Business Integrity that the action has been executed.
- A written confirmation of any disciplinary action taken, with the date of such completed action, shall be reported to Business Integrity.
- Business Integrity will record the disciplinary action taken in the Alert Registry.

- If the investigation report requires corrective actions (other than disciplinary actions):
  - Business Integrity will work with the relevant function management, and Human Resources as appropriate, to determine the appropriate corrective action (e.g., change in policies and procedures, in governance, in systems, in processes, additional training, reinforced monitoring, change in third parties, termination of contracts with third parties).
  - The relevant function management is responsible for implementing the corrective actions and confirming to Business Integrity that the actions have been executed.
  - A written confirmation of any corrective action taken, with the date of such completed action, must be reported to Business Integrity.
  - Business Integrity will record the corrective actions taken in the Alert Registry.
- The files relating to an alert are considered as closed only when all the disciplinary and/or corrective actions listed in the investigation report have been fully implemented.
- The person making the alert is informed on the fact that the alert has been processed and the investigation is closed.

5. REPORTS TO EXCO AND THE BOARD

- Business Integrity keeps the Executive Committee of Pharming Group N.V. informed on investigations and alerts, using aggregated and anonymised information.
- Business Integrity presents a summary (facts, observations, conclusion, resolutions, and corrective action to improve controls) and trends of alerts and disciplinary/corrective actions to the Corporate Governance Committee on a yearly basis, using aggregated and anonymised information. That summary will also be shared with the Board.
- Investigations related to financial matters, including incidents that may impact adopted financial statements, will be reported by Internal Control to the Audit Committee.