INTERNAL REPORTING SYSTEM POLICY

TABLE OF CONTENTS

1.- INTRODUCTION

In PLAIN CONCEPTS we are committed to compliance with the law and ethical and transparent behaviour in the development of our activity and relations with all Plain's staff, as well as with third parties (customers, suppliers…)

Our ethical principles include integrity, legality, transparency, and honesty, as well as a commitment to society and its development.

We always act in line with the aforementioned principles, which derives in a series of measures, such as the effective implementation of an Internal Reporting System.

2.- PURPOSE

The purpose of this Policy is to set out the characteristics and principles on which the Internal Reporting System is based, the main objective of which is enable Plain Concepts' employees and related third parties to report irregular or unlawful conduct of which they are victims or of which they have knowledge or reasonable suspicion.

The implementation of the Internal Reporting System has as its central focus the adequate protection against retaliation that the person who reports irregular or illegal conduct may suffer, and it is particularly important to establish a series of measures to ensure that protection is adequate.

On the other hand, the implementation of the Internal Reporting System within the company is also aimed at strengthening the compliance culture with the company.

3.- SCOPE OF APPLICATION

This Policy applies to all Plain concepts Group companies with respect to the Internal Reporting System, regardless of the geographic location of the Group Company affected by the constitutive violation that is contrary to the laws applicable to each of the Group Companies or contrary to the Plain Concepts Code of Ethics.

The implementation and management of the Internal Reporting System in Plain Concepts has been carried out following the parameters established in the Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements ad the fight against corruption, because the Parent Company of the Group (Plain Global Solutions, S.L.) and the Company with the highest business activity and manager of the Internal Reporting System (Plain Concepts, S.L.U.) have their registered offices in Spain.

However, the principles, guarantees, rights and procedures regulated in the legislation of each of the States in which the registered office of each of the Group companies is located shall be observed.

Specifically, the following is detailed:

- When the Companies affected are **Plain Global Solutions, S.L.; Plain Concepts, S.L.U**. and **Sidra Data Services, S.L.U**., Law 2/2023, of 20 February, *regulating the protection of persons who report regulatory infringements and the fight against corruption*, shall be applicable. The principles contained in this Law shall also apply when the Group companies concerned are not subject to a specific rule of the State in which they are located.

- When the company affected is **Plain Concepts GmbH,** *Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden*, shall be applicable (Law for better protection of whistleblowers and for the implementation of the Directive on the protection of persons who report breaches of Union law.)

- When the company affected is **Plain Concepts Benelux, B.V.,** Wet bescherming klokkenluider - *Wijziging van de Wet Huis voor klokkenluiders en enige andere wetten ter implementatie van Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 (PbEU 2019, L 305) en enige andere wijzigingen,* shall be applicable.

- When the company affected is **Plain Concepts RO, S.R.L.,** Lege nr.67 din 28 martie 2023, pentru modificarea art. 6 alin. (2) din Legea nr. 361/2022 privind protectia avertizorilor în interes public, shall be applicable.

The following areas will be taken into account to determine when a Group company is affected:

- **Material scope of application**

The material scope of application of this Policy in accordance with the provisions of Law 2/2023, is limited to:

- Any actions or omissions that may constitute infringements of European Union rights.
- Actions or omissions that may constitute a serious or very serious criminal or administrative offence. Th typology of actions includes, among others: actions or omissions that may constitute breaches of public procurement, money laundering

and terrorist financing, privacy, personal data, network security and information systems, public health, environmental protection, transport safety, consumer protection and labour law breaches in the area of health and safety at work.

- **Personal scope of application**

The provisions of this Policy shall apply to:

- Plain Concepts staff: employees, collaborators, and scholarship holders.
- Management and governing bodies.
- Persons working for or under the supervision and direction of Plain Concepts on an external basis.
- Third parties who have a relationship with Plain Concepts, such as suppliers and customers.

4.- INTERNAL REPORTING SYSTEM REQUIREMENTS

The Internal Reporting System complies with the requirements established in the law listed below:

1) It is designed, established, and managed securely, guaranteeing the confidentiality of the informant and of any third party involved, as well as of the actions carried out in the management and processing of the communication made.
2) It allows for the submission of written communications through a channel set up for this purpose.
3) It allows the submission of anonymous communications.
4) The Internal Reporting System is accessible to all the persons mentioned in point 3 of this document.
5) A procedure has been established for the management of incoming communications.
6) An Internal Reporting System Responsible has been appointed, with responsibility for the management of all aspects related to the System, as well as for the communication management procedure.
7) It is guaranteed that the communications submitted will be managed and processed effectively and efficiently in due time and form.

5.- INTERNAL REPORTING SYSTEM RESPONSIBLE

The Board of Directors of Plain Global Solutions, S.L., as the parent company of the Group (Governing Body) has appointed the Compliance Officer as the person responsible for the management of the "Internal Reporting System" for all the companies that constitute the Plain Concepts Group.

This appointment will be communicated to the Independent Information Authority or the Competent Authority in the matter.

The System Responsible performs his functions independently and autonomously from the rest of the Company's bodies, without receiving instructions in the performance of its duties and has the material and human resources to carry out his functions.

The System Responsible has proceeded to diligently process a specific procedure for the Management of the Internal Reporting System, which has been approved by the Governing Body.

6.- MEASURES FOR THE PROTECTION OF THE WHISTLEBLOWER

Persons who report any of the offences set out in point 3 of this document are entitled to protection provided that the following conditions are met:

a) They have reasonable grounds to believe that the information that is the subject of the communication is truthful, even if they do no at the time provide conclusive evidence.
b) The communication is based on facts that fall within the material scope of application set out in point 3 f this Policy.
c) The communication is made in good faith.

The prohibition of retaliation or discrimination against the whistleblower is established, for which purpose, the System Responsible and the Compliance Body shall adopt the necessary measures to achieve this goal.

If any situation of discrimination should arise with respect to the person who has made the communication of unlawful or irregular conduct, the System Responsible shall inform the Management and the persons in charge of managing the appropriate disciplinary measures.

7.- GOOD FAITH

One of the requirements for effective whistleblower protection is that the whistleblower always acts in good faith. A whistleblower is acting in good faith when:

- The communication made is based on facts or indications from which the commission of unlawful or irregular conduct falling within the material scope mentioned in point 3 of this document may be inferred or assumed.
- The whistleblower acts without intent to retaliate or to cause any damage to the reported person or to a third party.

In those case where a whistleblower makes communications in bad faith, falsely or in order to cause damage, disciplinary measures may be imposed or legal action, id appropriate, may be taken by us.

8.- CONFIDENTIALITY

Personal data of the whistleblower, the content of the communication, data of persons involved, as well as the communications maintained with the informant person in the process pf managing the procedure shall be confidential.

The procedure for communication through thew Internal Reporting System, which is located on our website, has security measures to preserve the confidentiality of the data.

The personal data and information relating to the communication made will only be know by the Responsible of the Internal Reporting System, as well as by the Compliance Body and professionals from the legal area in those cases which their collaboration is required in the management of the process. Likewise, there may be processes in which the collaboration and contribution of the specialised areas of the company is required, in which case they will only have access to the data that is strictly necessary and for the purpose of being able to carry out the process in an optimal way.

The Responsible of the system has the obligation of maintain the confidentiality about the identity of the whistleblower, as well as the person or persons to whom the communication is addressed (reported person) and third parties involved, except in those cases in which the competent authority requires the disclosure of the identity Independent Whistleblower Protection Authority, Courts…)

9.- PROCESSING OF PERSONAL DATA

The personal data processed in the management procedure of the communications made throughout its course, will be carried out at all times in compliance with the regulations in force and applicable to the matter, specifically with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (RGPD), Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), as well as Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties.

Access to personal data is limited to:

- The Responsible for the Internal System and persons who manage ot jointly with him/her.
- Head of the Human Resources Department.
- Responsible for the legal services of the entity or body, should legal measures be taken in relation to the facts.
- Data processors that may be appointed.
- The DPO.

If the processing of the procedure culminates in the finding of an irregular or unlawful act, the personal data will be communicated to the person assigned the functions of management and control of the sanctioning procedure within the company.

The **legitimacy** for the processing of personal data collected in the management of the communication process through the Internal Information system (Internal Channel) is covered in compliance with a legal obligation, which is contained in art. 6.1 c) RGPD, art. 8 of the LO 3/2018 (LOPDGDD) and art. 11 of the LO 7/2021.

In any case, the person concerned may at any time exercise their rights under the legislation that applies to personal data, the so-called ARCO rights (access, rectification, cancellation, and opposition).

The data collected referring to the whistleblower, third parties and the entire content of the communication will have the conservation period necessary to carry out the processing of the procedure and that established for legal purposes. If the communication is not admitted for processing, the data must be deleted immediately.

In any case, once three (3) months have elapsed since the receipt of the communication without any investigation actions having been initiated, the data must be deleted, unless the purpose of the conservation is to leave evidence of the operation of the system.

The Responsible for the System shall inform any person intervening in the procedure of:

a) The identity and data of the Responsible port he protection of personal data.

b) Personal data collected and their category.

c) Legitimation.

d) The storage period of the personal data.

e) Origin of the data.

f) Recipients to whom the data may be communicated (if applicable).

g) Rights to which he/she is entitled.

10.- REVIEW, MONITORING AND UPDATING OF THE POLICY

This policy will be subject to periodic review by the Compliance Body and the Human Resources Department in order to carry out any modifications and/or updates that may be necessary for its proper functioning and effectiveness, as well as to comply with legal provisions and our Code of Ethics.

11.- COMPLIANCE BODY

You may contact the Compliance Body, to report to the company any act that contravenes the provisions of this Policy or any questions you may have about its content, by sending an email to legal@plainconcepts.com

You are also welcome to comment on this policy and suggest ways to improve it.

12.- VALIDATION

In accordance with the procedure established, this policy has been validated by the Regulatory Compliance Committee.

13.-APPROVAL

This Policy shall not have retroactive effects prior to its entry into force, being approved by the Board of Directors and shall be applicable from the moment of its dissemination through the channels provided for this purpose.

14.- DISSEMINATION AND ENTRY INTO FORCE OF THE POLICY

This policy shall be communicated and disseminated to all the personnel of the Company and shall be available and permanently updated in the corporate Intranet or equivalent information hosting space of PLAIN CONCEPTS, being from that moment onwards of obligatory knowledge and compliance by all the personnel of the Company.

It will also be available and easily accessible in the Web Page, for the knowledge of any Group of Interest