ETHICAL CHANNEL PROTOCOL

CONTENTS

1. AIM AND PURPOSE 1
2. SCOPE OF APPLICATION 1
3. REPORTING OBLIGATION 3
4. WAYS OF REPORTING 3
5. PROCESSING REPORTS 6
   5.1. Procedure for receiving, tracking and investigating the complaint 7
   5.2. Investigation procedure 8
6. RIGHTS AND OBLIGATIONS 11
7. PROTECTION OF PERSONAL DATA 11
8. COMMUNICATION AND TRAINING 13
9. APPROVAL, APPLICATION AND REVIEW 14

1. AIM AND PURPOSE

Provital considers it essential to establish an internal reporting channel (Ethical Channel) so that employees and people or organisations that have links with Provital can communicate with the Ethics Committee in the event of a failure to comply with the organisation's rules and/or control mechanisms, or any breach of the principles set out in Provital'S Code of Ethics that could represent a risk for the company.

In order to comply with the Internal Reporting System it has implemented - hereinafter "the System" or "IRS" - and with Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption - hereinafter Law 2/2023 - PROVITAL S.A. has proceeded to set up a Reporting Channel so that all individuals falling within the scope of the aforementioned IRS can report cases of non-compliance or conduct contrary to the rules contained within the material scope of the organisation's IRS.
Consequently, the purpose of this Protocol is to regulate the functioning of the Reporting Channel, as well as the management and processing of the reports received and the investigative procedures to be initiated, where appropriate.

2. SCOPE OF APPLICATION

Material scope

The Reporting Channel set up by PROVITAL S.A. enables communication in relation to the matters described below, in compliance with Law 2/2023, of 20 February.

a) **Law 2/2023**:

- Actions or omissions which may constitute breaches of European Union law, provided that:
    - They fall within the scope of the European Union acts listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, on the protection of persons reporting breaches of Union law, irrespective of their status under national law;
    - They affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU);
    - They have an impact on the internal market, as referred to in Article 26(2) of the TFEU, including infringements of EU rules regarding competition and aid granted by States, as well as infringements relating to the internal market in connection with acts in breach of corporate tax rules or practices aimed at obtaining a tax advantage that would defeat the object or purpose of legislation applicable to corporate taxation.
- Actions or omissions that could constitute a serious or very serious criminal or administrative offence.
- Infringements of labour law in the area of health and safety at work.

b) **Preventing sexual and gender-based harassment**

- Any conduct contrary to current legislation on sexual and gender-based harassment (Organic Law 3/2007, on the effective equality of women and men, Article 48), as well as the provisions of the PROVITAL S.A. Protocol for the Prevention of Sexual and Gender-based Harassment.

c) **Preventing inequality for LGTBI people**

- Any conduct contrary to current legislation on equality for LGTBI people (Law 4/2023, of 28 February, on the real and effective equality of trans people and to guarantee the rights of LGTBI people), as well as the provisions of the PROVITAL, S.A. Protocol for dealing with harassment or violence directed at LGTBI people.

Personal scope

The protection specified in Law 2/2023, and the regulations established in this Protocol apply to the following informants:

a) Informants working in the private or public sector who have obtained information concerning offences in employment or in a professional context, including:
    - employees in the public or private sector;
    - the self-employed;
    - shareholders, partners and members of the administrative, management or supervisory bodies of a company, including non-executive members;
    - any person working for or under the supervision and management of contractors, subcontractors and supplier companies.

b) Informants who report or publicly disclose information on infringements obtained during an employment or statutory relationship that has already ended, volunteers, interns and trainees, whether or not they receive remuneration, as well as those whose employment has not yet started, in cases where the information on infringements was obtained during the recruitment process or pre-contractual negotiation.

c) The legal representatives of employees in the exercise of their functions of advising and supporting the informant.

d) Measures for protecting informants will also apply, where appropriate, to:
    - natural persons who, within the organisation in which the informant works, assist the informant in the process,
    - natural persons who are related to the informant and who may suffer reprisals, such as co-workers or relatives of the informant, and
    - legal entities for which the informant works, with which the informant has any other employment-related connection, or in which the informant has a significant shareholding. For these purposes, an interest in the capital or in the voting rights attaching to shares is deemed to be significant when it is sufficiently large to enable the person holding it to influence the legal entity concerned.

3. REPORTING OBLIGATION

All persons within the Provital organisation who are aware of any failure to comply with internal regulations or with the content of the Code of Ethics, with legal requirements or those related to criminal liability, or with any of the company's policies, procedures, protocols or controls (especially if it constitutes illegal or criminal conduct), are obliged to report it to our Ethical Channel as soon as possible via any means of communication.

4. WAYS OF REPORTING

In accordance with Law 2/2023, Provital has established the following ways of submitting reports through the Ethical Channel, so that they reach the Information System Management:

1) **Provital website Ethical Channel.** Internal channel with outsourced management.
2) **External Channel**. Independent Whistleblower Protection Authority channel.
3) **Public disclosure**.
4) **By post**. Internal management.
5) **Face-to-face interview**. Internal management.
6) **By telephone**. Internal management.

INTERNAL ETHICAL CHANNEL

Provital has set up an on-line tool, called "OVET AUKI", which anyone can access at: https://www.ovetauki.com/canal/provital

This channel is managed externally by the expert consultancy TARINAS VILADRICH ADVOCATS I PROCURADORS, SLP, and allows both anonymous and confidential reports, as preferred by the informant.

Operation and features

Access to the reporting channel is via the link https://www.ovetauki.com/canal/provital from any device at any time of the day, 365 days a year. The informant must complete the different stages of the report, following the instructions given by the platform itself, and must describe the facts in as much detail as possible, attaching all the evidence available, with a view to facilitating any subsequent investigation.

Please consult the OVET AUKI reporting channel user manual, attached as Annex III to this Protocol.

In the last stage of submitting the report, the informant must expressly choose whether he/she wishes the report to be confidential (and his/her identity therefore to be known) or to remain anonymous. If the informant chooses to be anonymous, he/she must keep the communication code generated in order to be able to access the OVET AUKI platform at a later date and check the status of the report, or to contact the body managing the channel or the organisation.

In case of queries or incidents, you can contact the technical service of the platform by e-mail at soporte@ovetauki.com

EXTERNAL CHANNEL

Any natural person may submit a report to the corresponding Independent Whistleblower Protection Authority channel, which in our case is the Anti-Fraud Office of Catalonia, via the link: https://denunciesanonimes.antifrau.cat/

PUBLIC DISCLOSURE

Public disclosure means making information available to the public regarding the actions or omissions specified in Article 2 of Law 2/2023.

Informants will be protected whenever any of the following conditions are met:

- Prior to public disclosure, the case has been reported through the above channels (internal, public and/or external) and appropriate measures have not been taken within the maximum time frame (3 months).
- There are reasonable grounds for believing that the infringement may constitute an imminent or manifest danger to the public, in particular where there is an emergency situation; there is a risk of irreversible damage, including danger to a person's physical integrity; or, when the external reporting channel has been used, there is a risk of retaliation or there is a low likelihood of effective treatment of the information, due to the particular circumstances of the case, such as concealment, destruction of evidence, collusion of persons in authority with the perpetrator of the infringement, or their involvement in the infringement themselves.

The conditions for the protection provided for in the previous paragraph do not apply when the informant has disclosed information directly to the press in accordance with the exercise of freedom of expression and truthful information provided for in the Constitution and in the legislation implementing it.

POSTAL ADDRESS

Reports may be submitted confidentially by sending a note or letter by post to the attention of Gema Soto Navarro, PROVITAL S.A. Internal Reporting System Manager (Ethics Committee) at C/ Gorgs Lladó, 200, 08210 Barberà del Vallès, Barcelona.

All reports received by post will be dealt with in a way that guarantees confidentiality and the rights of the informant. If the latter provides details of a means of communication, it will be used to inform them on the progress of the case or for any other necessary procedure or issue.

FACE-TO-FACE INTERVIEW

Informants may communicate in person with the System Manager within a maximum period of 7 days.
The conversation will be recorded and documented in one of the following ways, subject to the consent of the informant:

- by a recording of the conversation in a secure, durable and accessible format, or
- through a complete, accurate transcript of the conversation made by staff responsible for this procedure.

When submitting the report, the informant may indicate a postal address, e-mail address or safe place to receive notifications.

Data protection in accordance with Regulation (EU) 2016/679 and Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights will be guaranteed in all cases, and informants will be given the opportunity to check and rectify the transcript of the conversation and confirm acceptance by signing.
This channel will also allow for the submission and subsequent processing of anonymous reports.

TELEPHONE INTERVIEW

Informants have the option of communicating with the System Manager by telephone. To request this call +34 682 63 60 58.
Such communication must be recorded and documented in one of the following ways, subject to the informant's consent:

- by a recording of the conversation in a secure, durable and accessible format, or
- through a complete, accurate transcript of the conversation made by staff responsible for this procedure.

When submitting the report, the informant may indicate a postal address, e-mail address or safe place to receive notifications.
Data protection in accordance with Regulation (EU) 2016/679 and Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights will be guaranteed in all cases, and informants will be given the opportunity to check and rectify the transcript of the conversation and confirm acceptance by signing.
This channel will also allow for the submission and subsequent processing of anonymous reports.

5. PROCESSING REPORTS

This section applies to communications received by the organisation. Those processed by the Independent Whistleblower Protection Authority will be subject to that authority's statutes.

For reports submitted to Provital to be accepted as valid they must contain at least the following information:

- Description of the events.
- The evidence on which your suspicions are based.
- If known, the identity of the person(s) who committed the infringement and/or those who may have covered it up.
- If known, the place where the events occurred.
- Date at which the facts came to the informant's attention.
- How the informant came to know the facts (witnessing them, through third parties, through documentary evidence, etc.).

5.1. Procedure for receiving, tracking and investigating the complaint

Acknowledgement or proof of receipt

The informant must receive an acknowledgement of receipt or proof of receipt within 7 calendar days of submitting the report.

Filtering of incoming communications

The external manager of the information channel will be responsible for initial filtering of the report received, in order to assess whether (i) the informant is within the personal scope of Provital's Internal Reporting System and (ii) whether the communication falls within the material scope of the aforementioned System. In the case of anonymous communications, filtering will only apply to the material scope, as it is impossible to identify the informant.

Once the initial filtering has been completed, the following steps will be taken:

a) If the communication IS NOT within the personal and/or material scope of the IRS, the case will be closed, a report will be generated specifying the reason for closing it, and the informant will be notified and sent a copy of the report justifying the decision.
b) If the communication IS within the personal and/or material scope of the IRS, it will be checked to ensure it includes the minimum content mentioned above. If any of the information required to continue is missing, the informant will be contacted and asked to provide the missing information within 15 days.
    - If the missing information is not provided, the case will be closed and the informant will be notified and sent a copy of the report justifying the decision. This will not prevent the informant submitting a new report regarding the same situation.

- If the informant has not provided a method of contact, the investigation procedure will be initiated, recording what has happened and noting that the case may have to be closed if there is not sufficient information to carry out an appropriately diligent investigation.

c) If the report IS within the personal and/or material scope of the IRS and has the minimum required content, it will be necessary to verify whether the facts referred to in the communication are already under investigation or have already been investigated, and, if so, whether the informant provides new evidence or information that would justify opening a new investigation:
   - If the facts have already been investigated or are being investigated, and the informant DOES NOT PROVIDE evidence or new information, the case will be closed and a report drawn up indicating the grounds for the closure.
   - If the facts have already been or are being investigated, and the informant DOES PROVIDE new evidence or information, a new investigation will be initiated, taking into account this information and the findings of the investigation that has been or is being carried out in connection with the same events.
   - If the events have never been investigated, an investigation procedure will be initiated.

d) If the communication IS within the personal and/or material scope of the IRS, has the minimum required content, and is not related to a case that has already been or is being investigated, the entity that manages the channel will forward the communication to the body responsible for the IRS so that it may proceed, as soon as possible, to initiate the corresponding investigation. If the communication has been submitted by other means, it will be received directly by the IRS Manager.

5.2. Investigation procedure

Opening the case: the person who must initiate the investigation procedure is the designated IRS Manager, by means of an **initial report**, to which the information contained in the report received must be attached. This record must detail the reasons for which the case has been admitted for processing, the level of credibility of the report, and whether it is considered to have been made in good faith.

The **IRS Manager's own capacity** to carry out the investigation procedure should also be reviewed and, if necessary, the need to call on other people in the organisation or external experts, always following the procedure specified below in this Protocol, and respecting due process and the total confidentiality of the report received and the informant's identity. If necessary, the Manager may also appoint a person other than himself/herself to conduct the

investigation, either from within the organisation or externally, always respecting due process and confidentiality.

Investigative procedures should be established that allow for the preservation of evidence and respect the rights of employees. They may include interviews of a personal nature with specific departments in the organisation, or persons involved in the events reported. Professional services may also be required to assess the damage and the infringement, following the procedure for inviting external assistance described below.

It must also be determined **which departments or divisions need to be informed** about the investigation and at what reporting level, depending on: (i) the number of persons possibly involved and their position in the hierarchy (ii) the need to involve other departments.

Finally, the **need to inform the organisation's governing body** about the investigation should be assessed, depending on whether the governing body could be involved in the case or if doing so could lead to possible reprisals, which should be avoided in all cases.

Time limit for resolution: the time limits for completing the investigation, counted from notification of receipt of the communication, are as follows:

- For communications concerning the protection of European Union rights (Law 2/2023): **90 calendar days**.
- For communications regarding sexual or gender-based harassment (Organic Law 3/2007, on the effective equality of women and men and, specifically, according to the Spanish Ministry of Equality's protocol for the prevention of and action against sexual and gender-based harassment in the workplace, drawn up by the Subdirectorate General for Entrepreneurship, Equality in Business and Collective Bargaining, October 2021): **10 business days**.
- For communications regarding LGTBI equality (Law 4/2023, of 28 February, on the real and effective equality of trans people and to guarantee the rights of LGTBI people, and the Action Protocol for dealing with harassment or violence directed at LGTBI people): **10 business days**.

The time limit may be extended for a further 90 calendar days, but only in cases where the complexity of the investigation requires this and subject to a reasoned written justification.

Participation of external parties in the investigation

The IRS Manager should analyse the communication received and determine whether external parties should be asked to contribute to the investigation to ensure its success. Reasons why external parties may be invited to assist include:

- Lack of specific or technical knowledge of the events reported.
- A possible conflict of interest on the part of the IRS Manager.
- Good strategy when gathering evidence for the investigation, e.g. when interviewing staff, an outsider may be able to obtain more information than an insider.

In order to invite external parties to participate in the investigation, the IRS Manager should draw up a statement justifying the reasons. The party/parties must sign a declaration of absence of conflict of interest, attached to this Protocol as Annex I, and the confidentiality agreement attached to this Protocol as Annex II.

Resolution of the case and notification: at the end of the investigation, the IRS Manager will:

1. Draw up a **report on the investigation**, outlining all its stages and the evidence collected, with details of any issues that may have arisen and their resolution.
2. **Draw up a closure report** for the investigation, specifying the resolution adopted.

The possible outcomes of an investigation are as follows:

Case filed: this can occur for a number of reasons, for example:

- There is not enough information or evidence to investigate further.
- The informant's cooperation is needed to carry out the investigation and he/she refuses.

Case dismissed: when the result of the investigation is that the events described did not actually happen, or that the conduct is not contrary to the rules or legislation in force, or to policies implemented in the organisation.

Case referred to the relevant authorities: when it has been ascertained that the facts are credible and could constitute an offence as defined in the current Spanish Criminal Code, the case must be immediately referred to the Public Prosecutor's Office. Likewise, in cases where the IRS Manager deems it appropriate, he/she must refer the case to the relevant authority.

Internal resolution of the case, with or without sanction: when it has been proved that the events reported have indeed occurred, corrective action should be taken. The events may not constitute unlawful acts or may be minor offences, and appropriate action should be taken immediately. If corrective action cannot be taken immediately, a solution should be planned and implemented within a specific time frame. Consideration should also be given to the possibility of sanctioning the person(s) guilty of misconduct, an express, reasoned decision to this effect being recorded.

6. RIGHTS AND OBLIGATIONS

Reports must be submitted in good faith and measures will be taken to ensure that the informant is not subject to reprisals. In order to ensure that those reporting alleged misconduct in good faith are not subject to reprisals, communications should always be addressed to the System Manager. However, if the person who is the subject of the report should be the System Manager, it may be addressed to Ms MARTA ALVARO GARCIA, who will assume the role of IRS Manager exclusively with regard to the investigation of the report in question, respecting all the provisions of this Protocol.

The informant's identity will remain confidential or they will remain anonymous, as they prefer, unless they consent to the disclosure of their identity. This information will be treated as confidential in all cases. The System Manager may not disclose the identity of the informant under any circumstances, except to external (or internal) personnel involved in the investigation, when absolutely necessary. These persons must first sign the confidentiality agreement attached to this Protocol. However, in the event of a court order, the identity of informants will be revealed to the Judge, Public Prosecutor, Police or competent administrative authority, so that they are informed of the result of the investigation.

It is important to emphasise that the rights of the alleged perpetrator of the infringement do not include the right to know the identity of the complainant.
An informant may not be penalised or subjected to reprisals for submitting a report, provided this is done in good faith.

7. PROTECTION OF PERSONAL DATA

Part VI of Law 2/2023 establishes guidelines for the processing of personal data arising from the application of Law 2/2023, such data processing being governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights, and Organic Law 7/2021, of 26 May, on the protection of personal data treated for the purposes of prevention, detection, investigation and prosecution of criminal offences and the execution of criminal sanctions. Therefore: subjects must be informed about the processing of data, the exercise of their rights and the legal basis for the processing. No person may access data that would enable an informant to be identified, and the necessary technical and organisational measures must be in place to preserve the identity of informants and ensure the confidentiality of their data and/or their anonymity, if applicable.

Article 32 deals with the processing of personal data in the Internal Reporting System and it should be noted that access to data in the IRS is restricted to the following, according to their responsibilities and competences:

- The System Manager and whoever manages the System directly.
- The Human Resources manager or duly designated competent body, only when disciplinary action may need to be taken against a company employee.
- The legal services manager of the entity or body, if legal action is to be taken in connection with the events described in the communication.
- Persons responsible for data processing as designated from time to time.
- The Data Protection Officer.

Finally, the processing must be included in the Register of Processing Activity, in accordance with the provisions of Article 30 of the GDPR.

Data Controller: PROVITAL, S.A. CIF A-08584997
Pol. Ind. Can Salvatella – Gorgs Lladó, 200 - 08210 Barberà del Vallès (Barcelona-SPAIN)

Purpose: to manage the data of the informant in order to process the complaint submitted through the channel provided.

Legitimation:

- When it is compulsory to have an Internal Reporting System and in cases of internal communication, the processing of personal data will be considered lawful by virtue of the provisions of Articles 6.1.c) of the GDPR, Article 8 of the Organic Law on Protection of Personal Data and Guarantee of Digital Rights, and Article 11 of Organic Law 7/2021, of 26 May.
- The processing of personal data via external communication channels will be considered lawful in accordance with the provisions of Article 6.1.c) of the GDPR.
- The processing of personal data as a result of a public disclosure will be presumed to be covered by the provisions of Article 6.1.e) of the GDPR.
- If special categories of personal data are processed for reasons of essential public interest, the processing will be lawful in accordance with Article 9.2.g) of the GDPR.

International data transfers: no data are transferred internationally to third parties in countries outside the European Union.

Disclosure of data: data may be processed by other persons or even disclosed to third parties, if this is necessary for corrective measures to be applied within the organisation or for any appropriate disciplinary or criminal proceedings to be undertaken.

Data storage: the data processed may be kept in the information system only for the time necessary to decide whether an investigation into the facts reported should be undertaken. If it is established that the information provided or part of it is not truthful, it must be deleted as soon as this circumstance comes to light, unless this untruthfulness could constitute a criminal offence, in which case the information shall be kept for as long as necessary while legal proceedings take place. If 3 months have elapsed since the receipt of the communication and no investigation has been initiated, the data must be deleted, unless the purpose of retaining them is to provide evidence of the functioning of the system. Communications on which no action has been taken may only be stored in anonymised form. In this case, the obligation to block them, provided for in Article 32 of Organic Law 3/2018, of 5 December, is not applicable.

Rights of the persons concerned: data subjects may exercise their rights of access, rectification and deletion (the right to be forgotten), data limitation, data portability and opposition, by sending a letter to the attention of the Delegated Manager of the Internal Reporting System, Gema Soto Navarro, Pol. Ind. Can Salvatella - Gorgs Lladó, 200 - 08210 Barberà del Vallès (Barcelona), or sending an e-mail to info@weareprovital.com. They may also contact the competent data protection control authority (currently the Spanish Data Protection Agency), if they do not receive a satisfactory response and wish to file a complaint or obtain more information regarding any of these rights.

8. COMMUNICATION AND TRAINING

In order to guarantee the rights of those covered by this Protocol, and to ensure that they are aware of their obligations, PROVITAL S.A. staff must be provided with precise and unequivocal information about the existence of this Protocol.

Staff must be made aware of the existence of the reporting channel and how it may be accessed, at least by the publication of this information on the website.
The System Manager will coordinate and control the communication and training measures needed to ensure that everyone with links to PROVITAL S.A. is aware of the existence of the channel and how it works.

9. APPROVAL, APPLICATION AND REVIEW

This Protocol for the internal reporting channel was approved by Provital's Sole Director at the ordinary meeting held on 1 April 2024.

Notwithstanding the foregoing, this Protocol will be reviewed and, where appropriate, updated on an ongoing basis. In particular, it will be amended whenever there is scope for improvement.