INTERNAL REPORTING SYSTEM POLICY

CONTENTS

1. PURPOSE OF THE INTERNAL REPORTING SYSTEM POLICY

Opdenergy Holding, S.A. (hereinafter "**Opdenergy**" or the "**Organisation**") and group companies, within the framework of its Compliance Model and in accordance with the provisions of Spanish Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (hereinafter the "Whistleblower Protection Act"), has implemented an internal reporting system so that any member of Opdenergy or any unrelated third party that is aware of or suspects a regulatory breach may report it internally, providing their identity or anonymously.

The internal reporting system can also be used for internal queries concerning the regulations applicable to Opdenergy.

Opdenergy acknowledges all the principles set out in Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law and in the Whistleblower Protection Act and, in order to underline that commitment, has approved this Internal Reporting System Policy, the provisions of which are complementary to those set out in the Procedure for the management, investigation and response of communications received through the internal reporting system ("MIR Procedure").

The purpose of this Policy is to lay down the general principles of Opdenergy's internal reporting system, whistleblowers' rights and the procedure that regulates the process for bringing the matters referred to in the following section on the material scope of application to the attention of the IRS Officer.

2. MATERIAL SCOPE OF APPLICATION

This Policy provides the highest level of protection for individuals that report:

1) Actions or omissions that may constitute an infringement of European Union law, as defined by the Whistleblower Protection Act.
2) Actions or omissions that could constitute a serious or very serious criminal or administrative offence. All serious or very serious criminal or administrative offences involving pecuniary losses for the Public Treasury or the Social Security administration will be understood to be included.

The internal reporting system may also be used for the following purposes, although in these cases neither the whistleblower nor the report concerned will benefit from protection under the Whistleblower Protection Act or this Policy:

1) Reporting actions or omissions that may constitute a breach of the Company's internal regulations (which do not constitute a breach of European Union law or a serious or very serious criminal or administrative offence).
2) Conveying any queries related to the scope, fulfilment and interpretation of the Compliance Model and the internal regulations applicable in Opdenergy.

Communications strictly relating to employment or human resource policy issues (career development, remuneration, leave, etc.) or relating to professional performance are therefore excluded from the material scope of the internal reporting system. In such cases, the matter will be referred, if appropriate, to the Human Resources Area.

Furthermore, the internal reporting system should not be used to notify events that are immediately threatening to life or property. When emergency assistance is required, the situation should be reported to the emergency services.

3. PERSONAL SCOPE OF APPLICATION

This Policy covers not only Opdenergy's directors, officers and employees, but also such persons as volunteers, interns, trainees, candidates in selection processes, former employees or independent service providers, and worker representatives, as well as anyone working for or under the supervision and management of contractors, subcontractors and suppliers, and Opdenergy's shareholders.

The safeguards provided for in this Policy will also apply, where appropriate, to: (I) natural persons who, within the organisation in which the whistleblower is employed, assist the whistleblower in the process; (ii) natural persons who are related to the whistleblower and who may suffer reprisals, such as co-workers or relatives; and (iii) legal persons for whom he/she works or with whom he/she has any other relationship in an employment context, or in which he/she has a significant shareholding.

In addition, Opdenergy's internal reporting system may also be used by any Opdenergy's customers who are aware of or suspect regulatory non-compliance, and who will be subject to the level of protection expressly provided for in the Whistleblower Protection Act in relation thereto.

4. OBLIGATION TO REPORT NON-COMPLIANCE

Any member of Opdenergy or third-party professional working with the Organisation (in the terms set out in the previous section of this Policy) that becomes aware of any breach committed in an employment or professional context may immediately report it through the internal reporting system without fear of any kind of reprisal (in the case of persons forming part of the Organisation, such reporting is mandatory).

5. FUNCTIONS OF THE INTERNAL REPORTING SYSTEM OFFICER

The Board of Directors has appointed the Compliance Officer, in accordance with the current organisational structure and with the support of said Officer's team, as the person responsible for the internal reporting system, who is able to provide adequate guarantees concerning independence, confidentiality, data protection and communications secrecy.

6. INTERNAL REPORTING CHANNELS

Opdenergy has set up a confidential, protected internal reporting channel that complies with the requirements of the most stringent whistleblower protection and data protection regulations. This channel is managed through a platform (IT tool of the internal reporting system) and is accessible through:

- Opdenergy's corporate website: www.opdenergy.com
- The corporate intranet: https://opdefoto.sharepoint.com/sites/intranet/SitePages/Home.aspx

In addition, the whistleblower may ask the IRS Officer for a face-to-face meeting to provide the relevant information verbally, which must be held within a maximum of seven days of the request. The meeting will be duly documented in one of the following manners:

1) by recording the conversation in a secure, durable and accessible format, after telling the whistleblower that the communication will be recorded and that his/her data will be processed in accordance with the relevant regulations, or
2) through a complete and accurate transcript of the conversation made by the employees responsible for dealing with it. In addition, the whistleblower will be given the opportunity to

check, rectify and approve by signing the transcript of the conversation via the relevant platform (IT tool of the internal reporting system).

Whistleblowers may provide their identities or make their reports anonymously.

Such reports should, to the extent possible, contain the following details:

1) Full name of the person(s) to whom the events and/or conduct addressed in the report are attributed.
2) Date of the events and maximum available information on the events.
3) Any documents or other type of evidence at their disposal that may be used as proof of the occurrence of said events or conduct.

Apart from the above, any formal communication by a judicial body or a public administration will be considered a valid means of being informed of any such breaches.

In the event of any incompatibility or conflict of interest, i.e. if the person responsible for the reported events is the IRS Officer, the whistleblower may address the relevant notification to any member of the Management Committee, which will then assume, provisionally and for the sole purpose of dealing with the breach concerned, the functions of said officer.

7. EXTERNAL REPORTING AND PUBLIC DISCLOSURE CHANNEL

Notwithstanding the fact that the internal reporting channel is the preferred channel for reporting actions and omissions that constitute infringements of European Union rights or a serious or very serious criminal or administrative offense, any individual may directly utilise the external reporting channel provided in Spain by the Independent Whistleblower Protection Authority (A.I.I., according to its Spanish initials) or by the competent regional authority, if applicable.

The public disclosure of information on actions or omissions coming under the scope of this Policy will also imply the whistleblower's protection, provided that the whistleblower initially made the communication through internal or external channels, or directly through external channels, without appropriate action having been taken in this respect within the established timeframe, and provided that the requirements set out in the following section are also met.

8. WHISTLEBLOWER PROTECTION

Whistleblowers will be afforded all the safeguards provided for in this Policy and the MIR Procedure provided that:

1) They have reasonable grounds to believe that the information they report to Opdenergy is accurate at the time of communication and that the information falls within the material scope of the Policy.
2) They make the report or disclosure in accordance with the requirements provided for this purpose by Opdenergy and this Policy.

Persons who have publicly reported or disclosed information about actions or omissions covered by this Policy anonymously, but who have subsequently been

identified and meet the conditions set out in this paragraph, will be entitled to protection as provided for in this Policy.

Persons reporting to the relevant institutions, bodies, offices or agencies of the European Union on infringements falling within the scope of Directive (EU) 2019/1937 are entitled to protection in accordance with the provisions of this Policy.

Conversely, the protection set out in this Policy will not be afforded to persons who report or disclose:

1) Information contained in communications which have been rejected for any of the following reasons:
   a) The events reported lack any credibility.
   b) The events reported do not constitute a violation of the legislation covered by the scope of the Policy.
   c) The report is manifestly unfounded or, in the opinion of the IRS Officer, there are reasonable grounds to believe that it was obtained by criminal means. In the latter case, in addition to such rejection, a detailed account of the facts deemed to constitute an offence will be sent to the public prosecution service.
   d) The report does not contain significant new information on infringements referred to in a previous report in respect of which the relevant proceedings have been concluded, unless there are new factual or legal circumstances which justify a different treatment. In such cases, the IRS Officer will report the decision in a reasoned manner.
2) Information linked to complaints about interpersonal conflicts or involving only the whistleblower and the persons to whom the report or disclosure relates.
3) Information which is already fully available to the public or which constitutes mere hearsay.
4) Information relating to actions or omissions outside the material scope of this Policy.

The rejection of the report made through the authorised channels will be notified to the whistleblower, unless the communication was anonymous or the whistleblower had chosen not to receive notifications relating to the procedure.

9. PROHIBITION ON RETALIATION

Opdenergy will take the necessary measures to prohibit any acts of retaliation, including threats of and attempts at retaliation, against whistleblowers.

Retaliation means any acts or omissions which are prohibited by law, or which, directly or indirectly, entail unfavourable treatment solely because of their status as whistleblowers or because they have made a public disclosure. For purely informative purposes, the following are regarded as retaliation:

1) Suspension of employment, dismissal or termination of the employer-employee or statutory relationship.
2) Imposition of any disciplinary measures, demotion or denial of promotion and any other substantial change in working conditions.
3) Failure to convert a temporary employment contract into a permanent contract if the worker had legitimate expectations that he/she would be offered a permanent position.
4) Early termination or cancellation of contracts for goods or services.

5) Damage, including reputational damage, or pecuniary loss, coercion, intimidation, harassment or ostracism.
6) Negative evaluation or references regarding work or professional performance.
7) Blacklisting or dissemination of information in a particular sectoral area which hinders or prevents access to employment or to the contracting of works or services.
8) Refusal or revocation of a licence or permit.
9) Refusal to provide training.
10) Discrimination, or unfavourable or unfair treatment.

The measures set out in points 1 to 3 above will not be regarded as retaliation when they take place in the ordinary exercising of managerial authority under labour legislation due to proven circumstances, facts or infringements that are unrelated to the report submitted.

Likewise, any actions aimed at preventing or hindering the submission of reports and disclosures, and those that constitute retaliation or cause discrimination following the submission thereof, will be deemed null and void and, as appropriate, will result in disciplinary measures or the enforcement of liability, which may include relevant compensation for damages to the injured party.

Whistleblowers will also be entitled to the support measures provided in Spain by the Independent Whistleblower Protection Authority and/or regional protection bodies.

10. PROTECTION MEASURES AGAINST RETALIATION

The Organisation will take all necessary measures to ensure that whistleblowers are protected against retaliation. The main safeguards provided for in Directive (EU) 2019/1937 and the Whistleblower Protection Act are set out below:

1) Persons who report or publicly disclose information about the actions or omissions set out in paragraph 2, sub-paragraphs (1) and (2) of this Policy will not be deemed to have violated any restriction on the disclosure of information and will not incur any liability of any kind in connection with such report or public disclosure, provided that they had reasonable grounds for believing that the reporting or public disclosure of such information was necessary to notify an action or omission under this Policy. This measure will not affect criminal liability.

The provisions of the preceding paragraph cover the reporting of information by the workers' representatives even if they are subject to legal obligations concerning confidentiality or the non-disclosure of confidential information. The foregoing is without prejudice to the specific protection rules applicable under employment legislation.

2) Whistleblowers will not incur liability in respect of the acquisition of or access to information that is publicly reported or disclosed provided that such acquisition or access does not constitute a criminal offence.
3) Any other potential liability of whistleblowers arising from acts or omissions that are not related to the report or public disclosure or are not necessary to disclose an infringement will be enforceable under applicable law.
4) In proceedings before a court or other authority concerning harm suffered by whistleblowers, once the whistleblower has reasonably evidenced that he or she has made a report or public disclosure and suffered harm, it will be presumed that such harm occurred in retaliation for making the report or disclosure. In such cases, it will be for the person who has performed the harmful action to prove that it was based on duly justified grounds with no relation to the report or disclosure.
5) In legal proceedings, including those involving defamation, copyright infringement, breach of secrecy, breach of data protection regulations, disclosure of trade secrets or claims for damages based on employment law or by-law provisions, the persons making a report in accordance with this Policy will not have any liability as a result of protected communications or public disclosures. Such

persons will have the right to plead in their defence in such legal proceedings that they have made a report or public disclosure, provided that they had reasonable grounds for believing that the report or public disclosure was necessary to bring to light an infringement.

11. SAFEGUARDS FOR THE PERSONS REFERRED TO BY REPORTS

Opdenergy will ensure that the persons referred to by reports will be heard as part of the internal investigation, with a right to the presumption of innocence, right of defence and right of access to the file in accordance with applicable legislation.

Likewise, the identity of the person referred to by the reported breach will be protected and treated confidentially, as will the reported events, in the same way as the identity of the whistleblower, subject to such exceptions as may be necessary to ensure the proper performance of the investigation or any notification to the competent authorities.

12. PENALTIES

The penalties that may be imposed in each case will be those provided for in the Workers' Statute, in the applicable Collective Agreement or in applicable labour legislation and will be graduated based on the seriousness of the acts committed, and may take into consideration circumstances such as the damage or harm caused, any victims' circumstances, etc. Measures that are additional to disciplinary action may also be adopted, including applicable complaints or reporting the events to the appropriate administrative, police or judicial authorities.

In addition to possible breaches and penalties under employment legislation, the Independent Whistleblower Protection Authority may impose fines of up to €300,000 for conduct such as the following:

1) Preventing or attempting to prevent reports from being made or hindering or attempting to hinder their follow-up.
2) Taking retaliatory measures against whistleblowers.
3) Promoting abusive procedures against whistleblowers.
4) Breaching their duty to maintain confidentiality regarding the identity of the whistleblower or persons involved in the report, as well as their duty of secrecy regarding any information relating to it.
5) Publicly releasing or disclosing information known to be false.

13. CONFIDENTIALITY

Opdenergy guarantees the confidentiality of the identity of the whistleblower and of any third party mentioned in the report, and of the actions performed in managing and processing the report, as well as data protection and preventing access by unauthorised personnel.

Accordingly, access to data relating to a report is limited to members specifically authorised by Opdenergy to receive, monitor or resolve the reports received, and to third parties (e.g. a judicial authority, the public prosecution service or the competent administrative authority) when it constitutes a necessary and proportionate obligation imposed by applicable law in the context of an investigation carried out by the Spanish authorities or in the framework of judicial proceedings, in particular when disclosure is intended to safeguard the rights of defence of the person concerned.

In any event, except in the cases provided for, Opdenergy guarantees that no unauthorised person will be informed of the identity of the whistleblower or given any other information that could help to deduce, directly or indirectly, his or her identity. In particular, Opdenergy guarantees that the person

to whom the reported events refer will in no event be informed of the identity of the whistleblower or, as the case may be, of the person making the public disclosure.

Opdenergy will also ensure that the confidentiality of the data and events provided is safeguarded when the report is sent through reporting channels other than the established channels or to staff members who are not responsible for its processing. To this end, Opdenergy has adequately trained its staff in this area and has provided warnings concerning infractions derived from the nonfulfilment of the duty of confidentiality, and has also implemented the obligation of the report's recipient to immediately forward it to the IRS Officer.

In compliance with the foregoing, Opdenergy has implemented technical and organisational measures in its internal channels to protect the identity and guarantee the confidentiality of the data relating to the persons concerned and any third party mentioned in the information provided, particularly the identity of the whistleblower in the event that he/she has been identified.

With respect to the persons affected by a report, the Organisation will ensure that during the processing of the case these persons are entitled to the same protection as whistleblowers, safeguarding their identity and guaranteeing the confidentiality of the events and data involved.

Persons who receive public disclosures have the same obligations as described above and in no event will they obtain data allowing the whistleblower to be identified, and must have appropriate technical and organisational measures in place.

Disclosures made under this paragraph will be subject to the safeguards laid down in applicable law and, in particular, the whistleblower will be informed before his or her identity is disclosed, unless such information could compromise the investigation or judicial proceedings. When informing the whistleblower, the competent authority will send him or her a written explanation of the reasons for the disclosure of the confidential data concerned.

In any event, Opdenergy will ensure that any competent authorities receiving information on infringements involving trade secrets do not use or disclose them for purposes beyond what is necessary for the proper conduct of the proceedings.

14. DATA PROTECTION

The personal data processed under this Policy, including the exchange or transfer of personal data with the competent authorities, will be processed by OPDENERGY HOLDING, S.A. with registered office at c/ Cardenal Marcelo Spínola, 42, 5.ª planta, 28016 Madrid, and, if necessary, by the subsidiary of OPDENERGY HOLDING, S.A. to which the data subject belongs, as joint data controllers in accordance with data protection regulations (the "Joint Data Controllers").

Opdenergy has a data protection service channel that can be used by data subjects via email to privacy@opdenergy.com

The personal data provided through the internal system will be processed for the purpose of receiving and analysing the reported actions or omissions and, where appropriate, deciding whether to initiate an investigation into the reported events. In addition, certain information may be processed to provide evidence of the operation of the system. In the latter case, Opdenergy guarantees that the information stored as evidence will be anonymised.

If information is received that is not necessary for processing and investigating the actions or omissions referred to in Section 2 of this Policy, Opdenergy or, where appropriate, the Joint Data Controllers, will immediately delete it. Similarly, any personal data provided that refer to conduct that is not covered by the scope of the Whistleblower Protection Act and this Policy, as well as any information or part thereof that is proven to be untruthful, will be deleted, unless such untruthfulness constitutes a criminal offence.

Opdenergy and, where applicable, the Joint Data Controllers will process the personal data provided by the whistleblower in compliance with a legal obligation, i.e. in compliance with the Whistleblower Protection Act. Sensitive data may be processed by the data controller for reasons of essential public interest, in accordance with Article 9(2)(g) of Regulation (EU) 2016/679.

Personal data collected through internal channels will be retained in accordance with the provisions of applicable legislation. Specifically, such data will be kept only for the time necessary to decide whether to initiate an investigation into the reported events, which may not exceed three months from the date of receipt of the report. However, in the event that it is necessary to process the personal data for a longer period of time to continue an investigation or, where appropriate, because it is deemed necessary to initiate the appropriate legal actions, the data will be kept in an environment separate from the internal channels for as long as necessary to conclude the investigation or for Opdenergy and, where appropriate, its subsidiary to exercise the relevant actions.

For the above purposes, the Joint Data Controllers may provide access to personal data to:

1) Third-party service providers, such as consultants and external collaborators who provide support in the management or, as appropriate, investigation of reports received through internal channels.
2) Areas or departments involved in dealing with the report and, as appropriate, in the investigation and possible action to be taken with respect to the reported conduct where necessary.
3) In addition, personal data may be transferred to judges and courts, to the public prosecution service and to competent public bodies as a result of any investigation instigated.

The data subject is informed that, under the conditions established in the applicable regulations, he/she may exercise the rights recognised in data protection regulations by sending a letter to the attention of the Data Protection Department at its registered address or an email to the following address: privacy@opdenergy.com

The above notwithstanding, Opdenergy states that, should the person to whom the events reported or to whom the public disclosure refers exercise their right of opposition, it will be presumed that, unless proven otherwise, there are compelling legitimate grounds that legitimise the processing of their personal data.

Notwithstanding the whistleblower's rights under data protection regulations, in the case of oral communications, Opdenergy offers the opportunity to check, rectify and approve by signing the transcription of the conversation via the platform (IT tool of the internal reporting system).

Data subjects may also file complaints with the Spanish Data Protection Agency (www.aepd.es).

Opdenergy will regularly review the correct operation of its internal reporting system and the provisions of this Policy.

15. KEY PRINCIPLES OF THE MIR PROCEDURE

The MIR Procedure is governed by the following principles, which will be complied with when processing files:

- Confidentiality: The MIR Procedure will ensure the confidentiality of the identity of the whistleblower, of any third party mentioned in the report and of the data relating to the incident reported, except for communications with the judicial authorities, the public prosecution service or the competent administrative authority in the context of a criminal or disciplinary investigation.
- Impartiality: The IRS Officer must comply at all times with the principle of impartiality, treating all communications equally irrespective of the persons involved and avoiding any kind of conflict of interest.

- IRS Officer's independence: The IRS Officer will act with full independence and autonomy when deciding on the proceedings that he/she deems necessary to investigate the events reported, seeking to arrive at the truth in all cases.
- Documentation: Each report will generate a file in which the IRS Officer will include the detailed documentation of the entire investigation procedure.
- Good faith: The provisions of the MIR Procedure and this Policy will be interpreted in accordance with the principles and requirements of good faith.

16. COMMUNICATIONS LOG

Opdenergy will keep a record of all communications and enquiries it may receive through the internal reporting system, compiled in a log-book, complying at all times with existing confidentiality requirements and for the time that is strictly necessary and proportionate to fulfil European Union legal and regulatory requirements.

Opdenergy's Board of Directors.

MANAGEMENT, INVESTIGATION AND RESPONSE REPORTS RECEIVED VIA THE INTERNAL REPORTING SYSTEM

VERSION LOG

VERSION	DATE	SECTIONS	DESCRIPTION
01	13/11/2023	-	Newly edited document

Proposed:	Revised:	Approved:
Dámaso Alegre	-	-
C&S Director		Board of Directors

CONTENTS

1. PURPOSE

The purpose of this document is to lay down the general criteria and guidelines for managing, investigating and responding to reports received through the Internal Reporting System in the Opdenergy Group.

2. SCOPE

The scope of this document covers all companies, areas and subsidiaries of the Opdenergy Group (hereinafter Opdenergy or the Organisation).

3. REFERENCES

C-OPD-RC-EX-0004 Internal Reporting System Policy

Directive (UE) 2019/1937, the "Whistleblowing Directive"

Spanish Law 2/2023, the "Whistleblower Protection Act"

Other specifications and requirements to which the Organisation subscribes.

4. DEFINITIONS AND ACRONYMS

Internal Reporting System: A mechanism whereby employees or other interested parties may confidentially report any inappropriate or irregular conduct within the organisation. This system helps to strengthen the company's culture, promoting integrity and legal compliance.

5. ROLES AND RESPONSIBILITIES

ROLES	RESPONSIBILITIES
All Employees, irrespective of their position in the Organisation	Complying with the requirements set out in this document and collaborating in the proper operation of the Internal Reporting System.
Risk and Compliance Area	Developing the Internal Reporting System Officer in accordance with the approved statutes.

6. PROCESS DESCRIPTION

6.1 INTRODUCTION AND OBJECTIVES

Opdenergy Holding, S.A. ("Opdenergy" or the "Organisation") and group companies, within the framework of its Compliance Model and in accordance with the provisions of Spanish Law 2/2023 of 20 February regulating the protection of persons who report regulatory infringements and the fight against corruption (hereinafter the "Whistleblower Protection Act"), has implemented an Internal Reporting System so that any member of Opdenergy or any unrelated third party that is aware of or suspects a regulatory breach may report it internally, providing their identity or anonymously.

The Internal Reporting System can also be used for internal queries concerning the regulations applicable to Opdenergy.

Opdenergy acknowledges all the principles set out in Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law and in the Whistleblower Protection Act and, in order to underline that commitment, has approved this Management, Investigation and Response Procedure for reports received through the Internal Reporting System (the "MIR Procedure"), the provisions of which are complementary to those set out in the Internal Reporting System Policy.

This Procedure aims to regulate the use of the Internal Reporting System and the procedure for managing, investigating and resolving reports of possible breaches received, in accordance with the requirements of Directive (EU) 2019/1937 and the Whistleblower Protection Act.

6.2 SCOPE OF APPLICATION AND INTERNAL REPORTING CHANNELS ASSOCIATED WITH THIS PROCEDURE

This Procedure is associated with the internal reporting channels implemented by Opdenergy for reporting issues included in the material scope of application defined in Section 2 of the Internal Reporting System Policy.

The internal reporting channel provided by Opdenergy and associated with this Procedure has been implemented through a platform (IT tool) which is accessible via:

- Opdenergy's corporate website: www.opdenergy.com
- The corporate intranet: https://opdefoto.sharepoint.com/sites/intranet/SitePages/Home.aspx

In addition, whistleblowers may ask the IRS Officer for a face-to-face meeting to provide the relevant information verbally, which must be held within a maximum of seven calendar days of the request.

Apart from the above, any formal communication by a judicial body or a public authority will be considered a valid means of being informed of any such breaches. In addition, the internal reporting channels are open to third parties outside Opdenergy, particularly suppliers and customers.

6.3 EXTERNAL REPORTING CHANNEL OR PUBLIC DISCLOSURE

Notwithstanding the fact that the internal reporting channel is the preferred channel for reporting actions and omissions that constitute infringements of European Union rights or a serious or very serious criminal or administrative offense, any individual may directly utilise the external reporting channel provided by the Independent Whistleblower Protection Authority (A.I.I., according to its Spanish initials) or by the competent regional authority, if applicable.

6.4 PERSONAL CONFLICT OF INTEREST

In the event of any incompatibility or conflict of interest, i.e. if the person responsible for the reported events is the IRS Officer, the whistleblower may address the relevant notification to any member of the Management Committee, which will then assume, provisionally and for the sole purpose of dealing with the breach concerned, the functions of said officer.

6.5 CONFIDENTIALITY

All persons in Opdenergy with access to information, irrespective of the medium on which it is recorded and the form in which it was supplied, which is considered to fall within the material scope of the Internal Reporting System Policy and this Procedure, are aware that it is strictly confidential ("Confidential Information").

In any event, these persons undertake to keep secret and maintain the Confidential Information to which they have access in the strictest secrecy, particularly information considered to be of a personal nature or, where appropriate, the identity of the whistleblower. Furthermore, the members of the body responsible for the system will use the Confidential Information only for the performance of the functions entrusted to them and in strict compliance with the Internal Reporting System Policy and this Procedure. They further undertake to ensure the integrity of the information contained in the internal channel and not to give their passwords or user names for applications and systems owned by Opdenergy to any third party.

In compliance with applicable regulations, the identity of the whistleblower may only be notified to the judicial authorities, the public prosecution service or the competent administrative authority in the context of a criminal or disciplinary investigation.

Failure to comply with this obligation by persons having access to Confidential Information may be grounds for disciplinary dismissal or other penalties under the provisions of the Workers' Statute, the applicable Collective Agreement or applicable employment legislation, and they will be liable for any damage that Opdenergy or the whistleblower may suffer as a result of the failure to comply with this obligation.

6.6 SAFEGUARDS FOR PERSONS CONCERNED BY REPORTS

Opdenergy will ensure that the persons referred to by reports will be heard as part of the internal company investigation, with a right to the presumption of innocence, right of defence and right of access to the file in accordance with applicable legislation.

Likewise, the identity of the person referred to by the reported breach will be protected and treated confidentially, as will the reported events, in the same manner as the identity of the whistleblower, subject to such limits and exceptions as may be necessary to ensure the proper performance of the investigation or any notification to the competent authorities.

6.7 RECEIPT OF REPORTS AND GENERATION OF FILES

6.7.1 ACKNOWLEDGEMENT OF RECEIPT

Following receipt of a report through internal reporting channels, the IRS Officer will acknowledge receipt thereof within seven calendar days, unless such action could jeopardise the confidentiality of the communication.

The acknowledgement of receipt will include some preliminary information on personal data processing in accordance with Article 11 of Spanish Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guaranteeing of Digital Rights. In addition, the person concerned will be told where to find information on the processing of his/her personal data.

The whistleblower will also be expressly informed that his or her identity will be protected and will not be revealed to the persons to whom the alleged breach relates or to third parties.

6.7.2 REQUEST FOR ADDITIONAL INFORMATION

In the event that the information received is considered insufficient, the IRS Officer, when acknowledging receipt or at a later date, will request further information from the whistleblower. The request for additional information should mention the specific aspects of the information provided that need to be expanded upon. At this stage it will not be necessary to provide very detailed information on the reported breach, but only that which is strictly necessary for the creation and preliminary management of the file.

6.7.3 INITIAL FILE GENERATION

With the information received and the corresponding acknowledgement of receipt, the IRS Officer will form an individual file for each case which will be suitably numbered and classified with an identification code and the date of registration.

In the event that various reports are received on the same or related events, the IRS Officer may join them in a single file.

6.8 PRELIMINARY ANALYSIS AND DECISION ON THE REPORT RECEIVED

6.8.1 PRELIMINARY ANALYSIS OF THE REPORT RECEIVED

The IRS Officer will carry out a preliminary analysis to verify the substance, sufficiency and plausibility of the information, the credibility of the whistleblower and the relevance of the events reported, determining whether they could constitute an infringement of European Union law, a serious or very serious criminal or administrative offence, or a breach of internal regulations.

For this preliminary analysis and for the other phases defined below, legal advice may be sought from Opdenergy's external legal advisers if the matter is regarded as having a high degree of factual or legal complexity.

6.8.2 PRELIMINARY DECISION ON THE INFORMATION RECEIVED

Depending on the outcome of the preliminary analysis, the IRS Officer will take one of the following decisions, recording a reasoned report:

a) Rejection of the report and immediate closure of the file in the following cases:
   - The reported events do not come under any of the cases referred to in the material scope of the Internal Reporting System, as defined in Section 2 of the Internal Reporting System.
   - The report is a mere reproduction of a previous report

   that was rejected or was or duly investigated, without any new information being provided.
   - The content of the report is manifestly irrelevant or the reported events

   are implausible, or the whistleblower lacks any credibility.

- The information is insufficient to take any further action.

b) Admission of the report and opening of an investigation in relation to the events reported, in accordance with the provisions of this Procedure.
c) Immediate transfer of the information to the public prosecution service when the events reported may be indicative of a criminal offence, or to the European Public Prosecutor's Office when the events concern the financial interests of the European Union.

6.8.3 INFORMATION PROVIDED TO THE WHISTLEBLOWER ON THE FILE

In all the cases described above, the IRS Officer will inform the whistleblower of the rejection or admission of the report and any additional measures taken, unless the report is anonymous or the whistleblower has chosen not to receive any notifications.

6.8.4 ADDITIONAL MEASURES

In parallel to the adoption of the decisions described in section 6.8.2 above, the IRS Officer may adopt, following the procedure laid down in the Collective Agreement or in employment legislation, any measures that, in view of the reported breach, are considered necessary to strengthen the prevention and control systems in place at Opdenergy.

6.9 INVESTIGATION PROCEDURE

When a decision is taken to initiate an investigation procedure in accordance with section 6.8.2.b), the following steps will be taken:

- Choosing the investigation strategy (see section 6.9.1).
- Planning the investigation (see section 6.9.2).
- Notifying the parties concerned (see section 6.9.3).
- Conducting the investigation (see section 6.9.4).
- Documenting the investigation procedure (see section 6.9.5).
- Drawing up the final report (see section 6.9.6).
- Final measures (see section 6.9.7)

6.9.1 CHOICE OF INVESTIGATION STRATEGY

Depending on the context, scope and persons allegedly involved in the breach in question, the IRS Officer will assess the investigation strategy to be implemented in the specific case, and may choose one of the following options:

a) The investigation procedure will be entirely designed, led and managed by the IRS Officer, notwithstanding any consultations or support that may be required from other departments for complete substantiation. These departments are expressly required to provide the IRS Officer with any information requested in their possession or of which they are aware.
b) The investigation procedure will be designed, led and managed by an investigation team appointed by the IRS Officer for this purpose, whose members may include representatives of the divisions, areas or departments likely to have knowledge of the alleged events or whose involvement may be relevant for the purposes of the investigation.
c) The investigation procedure will be delegated to a specific internal body or department in the company when this is advisable in view of its speciality or specific expertise required for the investigation.
d) The investigation procedure will be fully or partly outsourced, depending on whether the circumstances of the case require expert advice on a particular matter or a full investigation

by a party external to Opdenergy. The choice of this strategy will be particularly advisable in cases where it is considered that the investigation may require a special standard of confidentiality.

Furthermore, all persons forming part of the investigation team are obliged to keep the whistleblower's identity secret, and to sign a confidentiality agreement specific to each case.

It is particularly important that if any conflict of interest exists involving a member of the specific team appointed for the investigation due to said member's involvement in the events reported, that member must withdraw from the investigation and may not take part in it.

6.9.2 INVESTIGATION PLANNING

Both the IRS Officer and any other designated investigator will plan the investigation with the aim of clarifying the events that took place and identifying those responsible. This planning may include the following components:

a) Identifying the legislation, policies, procedures or internal regulations involved, as well as the reputational, economic, financial or legal risks that could result from the alleged breach.
b) Identifying all information and documents that may be relevant and which it could be useful to review (emails, websites, the company's audiovisual surveillance and security records, lists of attendees, passwords or electronic security devices, accounting evidence, etc.). In the event of access to any document that is not strictly professional and could contain personal content, access should be made prudently and as non-intrusively as possible (always taking into account criteria of suitability, necessity, usefulness and proportionality), ensuring the chain of custody. In the event of any uncertainty, Opdenergy's legal advisors should be consulted.
c) Determining, if necessary and with the collaboration of the Human Resources Area, the need and, where appropriate, the urgency of adopting precautionary measures with respect to the persons concerned by the report. Such precautionary measures are not limited to, but may include, the following:
   - Transferring the parties under investigation to another division, area or department or temporarily relocating them.
   - Altering the usual tasks or responsibilities of the parties concerned by the report.
   - Suspending said parties immediately.
d) Defining the steps to be followed in the investigation and at the meetings with the persons concerned in order to ensure its proper implementation, identifying the interlocutors to be interviewed, questions to be asked, possible witnesses to the event reported, etc.
e) Including in the investigation file all the information that may be of interest in relation to the working life of the person concerned in Opdenergy (employment record, previous contingencies, company policies, procedures and regulations particularly applicable to said person, etc.).
f) In planning the investigation, efforts should always be made to ensure:
   - The objectivity and fairness of the process;
   - The privacy of the persons under investigation; and
   - The minimisation of the impact of the investigation.

6.9.3 NOTIFICATION TO THE PERSONS CONCERNED

Prior to initiating the investigation, the designated investigator will contact the parties referred to in the report, identifying himself as the person responsible for investigating the alleged breach, briefly informing them of the actions attributed to them and of the main milestones expected to arise during

the investigation. The person concerned will be informed of his or her right to make written submissions and of the processing of his or her personal data, and may be heard at any time.

The above steps will be taken unless, in the investigator's opinion, and in order to prevent the destruction and/or concealment of evidence or otherwise undermine the investigation, the person concerned should be notified at a later stage and, in any event, when a statement by the person concerned is required at the hearing stage or before the termination of the investigation process.

In no event will the identity of the whistleblower be disclosed to the person concerned, nor will access to the report be allowed.

Notwithstanding the right to present written submissions, the investigation will, whenever possible, include an interview with the person concerned in which, with full respect for the presumption of innocence, said person will be invited to explain his/her version of the events and to provide such evidence as he/she considers appropriate and relevant.

6.9.4 CONDUCT OF THE INVESTIGATION

The investigation will include all investigative measures that are deemed necessary to establish the facts, the persons responsible and any corrective measures to be taken. The investigation will be conducted at all times with the utmost respect for the duty of confidentiality and protection of the whistleblower and respecting in all cases the presumption of innocence, the right to be heard and the right to honour of the person concerned by the report.

The following are some of the main steps that may comprise the investigation:

a) Conducting an interview with the whistleblower to obtain further information on the report made.
b) Declaration of the parties concerned by the report.
c) Arranging questionnaires and interviews with witnesses.
d) Arranging interviews with the superiors and colleagues of the persons concerned and with any other persons deemed necessary.
e) Collecting as much information as possible through Opdenergy documentation.
f) If such proves essential to determine the facts, adopting surveillance measures through detectives or computerised, telematic or audiovisual means, provided that they meet criteria of reasonableness, suitability and proportionality, ensuring at all times the worker's right to privacy and the right to the confidentiality of the relevant communications.
g) Seeking external assistance from other professionals.
h) Any other steps that the investigator deems necessary to determine the facts, including, where deemed necessary, communications with and requests for additional information from the whistleblower.

As a general rule, the duration of the investigation proceedings may not exceed three months from the date of receipt of the report. Exceptionally, in particularly complex cases, the deadline may be extended by a maximum of three additional months.

6.9.5 DOCUMENTATION OF THE INVESTIGATION PROCEDURE

The file must include detailed documentation of the entire investigation procedure, including the investigation plan initially drawn up, all the documents obtained and the minutes of interviews held.

All interviews conducted will be duly documented, either by means of a complete and accurate transcript prepared by the investigator and signed by both the interviewees—after offering them the opportunity to check and correct it—and the investigator, or by means of a recording in a secure,

durable and accessible format, after notifying the interviewee that the communication will be recorded and informing him/her of the processing of his/her data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016. Interviewees will also be informed that the collection, processing and disclosure of personal data will comply with prevailing personal data legislation.

6.9.6 FINAL REPORT

Once all the steps of the investigation have been completed, the investigator will prepare a report on the findings which will include a brief description of the following items:

a) Nature of the contingency: To the extent possible, the parties involved, the nature of the events, the date, place and circumstances in which they allegedly occurred and the legal provisions or internal rules allegedly breached will be identified, including a statement of the facts reported together with the identification code of the report and the date of registration.
b) Identity of the investigator: The member(s) of the work team responsible for carrying out the investigation will be identified.
c) Classification of the report to ascertain whether or not it is considered priority.
d) The actions carried out in order to verify the plausibility of the alleged events.
e) List of relevant facts and findings: The most relevant facts identified in the course of the investigation procedure will be reported, differentiating them by the source of information from which they were identified, for example:
   - Opdenergy document,
   - information provided by the whistleblower, or
   - information obtained from interviews with the persons concerned and with witnesses.
f) Conclusions and assessment of the facts: The conclusions drawn by the investigator and the evidence supporting them, as well as the investigator's assessment of the reported events, will be specified and two possible courses of action may be proposed:
   - Proposal to continue the procedure if it is considered that, on the basis of the actions performed, it has been sufficiently accredited that the person concerned has committed any of the infringements laid down in Section 2 of the Internal Reporting System Policy.
   - The procedure will be shelved if it is considered that none of the infringements referred to in Section 2 of the Internal Reporting System Policy has been committed, if the perpetration thereof is not sufficiently evidenced or if the perpetrator has not been identified. The whistleblower and, if appropriate, the person concerned will be informed of this decision.
g) Penalty proposal: If the investigator's report concludes with a proposal to continue with the procedure, the report must include a final section identifying the penalties that may be imposed by Opdenergy against the perpetrators of the alleged breach and any other additional measures, including compensatory actions that might be taken in relation to any injured party.

6.9.7 FINAL MEASURES

The final investigation report must be immediately forwarded to the Management Committee once completed.

The final investigation report will be filed together with the rest of the investigation file.

6.10 CONCLUSION OF THE PROCEDURE

6.10.1 RESPONSIBLE BODY

The Management Committee is the competent body to deal with any non-compliance that may occur in Opdenergy and decide on the investigator's proposals.

However, in the event that a member of Opdenergy's Management Committee is involved in the investigation, he/she must refrain from participating in the part of any meeting(s) where this matter is discussed.

6.10.2 HEARING PHASE

Upon receipt of the final investigation report, the Management Committee will forward it to the person concerned by the investigation who will be given five days in which to submit, in writing or orally, any arguments he or she deems appropriate and to provide any documents he or she deems relevant.

6.10.3 MANAGEMENT COMMITTEE'S DECISIONS

After the time limit for the party concerned to present their allegations has expired, the Management Committee may take one of the following decisions:

a) Admit or disallow the evidence submitted by the person concerned, giving reasons.
b) Request additional investigative steps by the investigator.
c) Archive the file for lack of sufficient evidence or because the facts are irrelevant for these purposes, returning it in this case to the IRS Officer to be archived.
d) Declare that a breach has been committed in Opdenergy and impose any penalty or take any additional measure deemed appropriate.
e) If it is determined that the facts of the case could be indicative of a criminal offence once the final report has been issued, the information obtained in the investigation will be immediately forwarded to the public prosecution service. If these facts affect the pecuniary interests of the European Union, the information will be forwarded to the European Public Prosecutor's Office.

6.10.4 PENALTIES

The penalties that may be imposed in each case will be as provided for in the Workers' Statute, in the applicable Collective Agreement or in applicable employment legislation.

The amount of these penalties will depend on the seriousness of the acts committed and may take into consideration circumstances such as repeated non-compliance, the damage or harm caused, the circumstances of any victims, etc.

The application of penalties will be handled by the Human Resources Area.

6.10.5 OTHER MEASURES

The Management Committee may take additional reaction and response measures, such as:

a) reporting the case to a competent administrative or judicial authority;
b) assessing previous evidence of similar breaches and ensure that appropriate action is taken to understand the cause of the breach;
c) taking compensatory action for any person or entity that might have been harmed by the events;

d) establishing processes, procedures and control mechanisms to prevent any similar breach and propose organisational or preventive measures of any kind;
e) taking decisions related to internal communication, training or dissemination of the facts, at the level of the unit concerned (division, area or department) or at a general level (all employees) when this is considered an effective tool for preventing similar breaches in the future (complying at all times with data protection regulations);
f) taking appropriate action against anyone making a false report, i.e. in the knowledge that the events reported are false.

6.10.6 NOTIFICATION OF DECISIONS

The decisions of the Management Committee will be notified immediately and in writing to the persons concerned.

The decisions will also be notified to the superiors of the persons concerned and the whistleblower. The notification to managers or the whistleblower must omit any information on the nature of the procedure followed or the events reported, in compliance with data protection regulations.

Finally, the Management Committee's decisions will be passed on to the IRS Officer to be processed and filed, and for any measure taken to be monitored.

6.11 DOCUMENT RETENTION

6.11.1 RETENTION PERIODS

The data processed may be retained in the internal channel only for the time necessary to decide whether to open an investigation into the facts reported.

If it is established that all or part of the information provided is untrue, it must be deleted as soon as this becomes known, unless such lack of truthfulness constitutes a criminal offence, in which case the information will be kept for the time necessary during the relevant legal proceedings.

In any event, if no investigation is initiated within three months of the report being received, the report must be deleted, unless the purpose of its retention is to provide evidence for the functioning of the system.

Reports that have not been processed may only be recorded in anonymised form, without the blocking obligation provided for in Article 32 of Spanish Organic Law 3/2018 of 5 December being applicable.

6.11.2 COMMUNICATIONS LOG

Opdenergy will keep a record of all communications and enquiries it may receive through the Internal Reporting System, compiled in a log-book, complying at all times with existing confidentiality requirements and for the time that is strictly necessary and proportionate to fulfil European Union legal and regulatory requirements.

The IRS Officer will record the reports received, including the following information:

- File number.
- Date of the acknowledgement of receipt issued by the IRS Officer.
- Statement by the IRS Officer following a preliminary analysis of the report.
- Final report prepared by the investigator.
- Management Committee's resolution.

Where the communication has been made orally, Opdenergy reserves the right to document the oral complaint in one of the following ways:

i. By recording the conversation in a durable and accessible format.

ii. Through a complete and accurate transcript of the conversation made by the investigator.

In any case, the whistleblower will be entitled to verify, rectify and sign the transcription as acceptance.

When the whistleblower has requested a personal interview with the IRS Officer to make the report, Opdenergy will ensure, subject to the whistleblower's consent, that complete and accurate records of the meeting are kept in a durable and accessible form.

Access to all or part of the contents of the log-book may only be granted under an order from the competent judicial authority, within the framework of judicial proceedings and under its supervision.

The data contained in this log-book will be kept for the time that is strictly necessary, and in no event for more than 10 years.

6.12 RESOLUTION OF QUERIES

All Opdenergy members who have any doubts or concerns in relation to the regulations applicable to Opdenergy may submit their queries through the internal reporting channels.

Upon receipt of a written query, the IRS Officer will acknowledge receipt within seven calendar days and will respond in writing within ten calendar days.

If the query is made verbally, the IRS Officer will record it in writing and will also reply in writing within 10 calendar days.

If the query is complex or has implications that require a detailed analysis for its resolution, these time limits may be extended by the time necessary, with prior notification to the person making the query.

Notwithstanding the above deadlines, the IRS Officer will respond to queries as rapidly as possible, taking into account the urgency and complexity of the query.

The IRS Officer will record the queries received, duly anonymised and in compliance with prevailing data protection regulations.

The queries received will also be filed in the log-book described in section 6.11.2 above of this Procedure, and the Management Committee will be informed thereof.

Any personal data collected for the response to the query will be processed in accordance with paragraphs 6.5 and 6.13 of this Procedure.

6.13 PERSONAL DATA PROTECTION

In compliance with applicable regulations, the Internal Reporting System Policy and this Procedure, access to personal data contained in internal channels will be restricted, within the scope of their authority and functions, exclusively to:

a) the IRS Officer and whoever manages it directly;
b) the human resources manager or the duly designated competent body only when disciplinary measures against an employee are applicable;
c) Opdenergy's legal counsel, if legal action is to be taken in relation to the reported events;
d) any data processors appointed;

e) where applicable, the Data Protection Officer.

The processing of the data by other persons or their communication to third parties will be lawful when necessary for the adoption of corrective measures by Opdenergy or the processing of any applicable penalty or criminal proceedings.

Under no circumstances will personal data be processed if they are not necessary for ascertaining and investigating the actions or omissions referred to in the Internal Reporting System Policy and in this Procedure, and they will be immediately deleted. Any personal data that might have been communicated and relate to conduct that does not fall within the scope of the Whistleblower Protection Act, the Internal Reporting System Policy or this Procedure will likewise be deleted.

If the information received contains personal data included in special data categories, it will be deleted immediately without being recorded or processed.

7. APPENDICES AND REGISTRATION FORMATS[1]

P-OPD-IN-RC-0001-R01 Internal Reporting System Tool

1 The registration formats may be replaced by other formats at the request of data subjects or due to business needs, but the minimum stipulated information must always be included in them.

Place and date

Employee’s signature

Employee’s name