INTERNAL REPORTING SYSTEM POLICY

doValue

Table of Contents

1. VERSION CONTROL

VERSION CONTROL	
Company	doValue Spain Servicing, S.A.U. and its subsidiaries
Title	Internal Reporting System Policy
Version	V.3.0
Document	Policy 6
Prepared by	Compliance Officer
Approval Date	31/07/2026
Party responsible for approval	Board of Directors of doValue Spain
Ratification date	09/2026
Party responsible for ratification	n/a
Policies or rules amended / repealed	Internal Reporting System Policy v.2
Version changes	Various sections are updated in order to align them with the recommendations of the AIPI and certain nuances of Law 2/2023 In addition, the main time limits provided for in Law 2/2023 are incorporated.
Date of last update	31/07/2026

Version	Reason for the Change	Responsible party	Approval date	Ratification date
1.0	Initial version	Regulatory Compliance	16/06/2023	16/06/2023
2.0	Version 2: - Replacement of the Head of the Internal Reporting System by a collegiate body to be known as the Internal Reporting System Committee (CSII), and consequent adjustments. - Section 4. now includes the purpose of the Internal Reporting System, access to and operation of the internal reporting system and the external reporting channels. - Section 5. now includes the principle prohibiting retaliation	Regulatory Compliance	16/03/2026	16/03/2026

	against Reporting Persons and Related Third Parties.			
3.0	Various sections are updated in order to align them with the recommendations of the AIPI and certain nuances of Law 2/2023. In addition, the main time limits provided for in Law 2/2023 are incorporated.	Compliance Officer	31/07/2026	09/2026

2. PURPOSE

The purpose of this Policy is to establish the principles, responsibilities and general rules governing the operation of the Internal Reporting System (hereinafter, the **"SII"**) of doValue Spain Servicing, S.A.U. (hereinafter, jointly, **"doValue"**, "**DVSP**", the **"Organisation"** or the **"Company"**) and its subsidiaries.

The SII constitutes the preferred channel for the reporting and management of information on acts or omissions that may constitute infringements of European Union law, serious or very serious criminal or administrative offences, breaches of the Code of Conduct or of the applicable internal regulations, as well as any other conduct contrary to the ethical and compliance principles of the Organisation.

Likewise, this Policy establishes the principles of action, the guarantees for the protection of reporting persons and other persons concerned, as well as the measures intended to ensure the confidentiality, independence, absence of retaliation and appropriate management of the reports received through the Internal Reporting System.

This Policy implements the requirements established in **Law 2/2023, of 20 February**, regulating the protection of persons who report regulatory infringements and the fight against corruption, and is supplemented by the **Internal Reporting System Management Procedure**, which governs the operational functioning of the system and the processing of the reports received.

3. COMMITMENT OF THE ORGANISATION

doValue and its subsidiaries maintain a firm commitment to ethics, integrity, transparency and regulatory compliance as fundamental principles of their corporate governance model and of their organisational culture.

Within this framework, the Organisation promotes an environment in which all persons may report, in good faith and without fear of retaliation, any conduct, act or omission that could be contrary to the applicable legislation, to the Code of Conduct or to the Organisation's internal regulations.

In order to reinforce those principles and to facilitate the early detection of possible breaches, the Board of Directors of doValue Spain Servicing, S.A.U. has implemented an Internal Reporting System and approved this Policy, making available to stakeholders appropriate channels for the receipt and management of reports, ensuring at all times confidentiality, the protection of reporting persons, impartiality in the management of investigations and respect for the rights of all persons involved.

Likewise, the Organisation expresses its commitment to the prohibition of any form of retaliation against those who, acting in good faith and on reasonable grounds, report or disclose information on possible infringements, promoting a culture based on accountability, trust and the continuous improvement of control and compliance systems.

The Organisation shall adopt the measures necessary to ensure the proper functioning of the Internal Reporting System, the availability of the resources required for its effective management and compliance with the requirements established in the regulations applicable at any given time.

4. SCOPE OF APPROVAL, APPLICATION AND UPDATES

4.1. Approval

This Policy forms part of the Internal Reporting System of doValue and its subsidiaries and is approved by the respective governing bodies of the companies required to apply it, in accordance with the provisions of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption.

Likewise, the governing bodies shall be responsible for the appointment and, where applicable, the removal of the Head of the Internal Reporting System, as well as for the general supervision of its proper functioning.

4.2. Application

This Policy is binding on doValue and its subsidiaries, as well as on all members of the Organisation, including the members of the governing bodies, executives, employees, temporary agency workers, interns, trainees and any other person who carries out their professional activity under the direction, supervision or control of the Organisation.

Likewise, the Organisation shall promote awareness of and compliance with the principles contained in this Policy on the part of suppliers, contractors, external collaborators, business partners and any third parties with which it maintains professional or commercial relationships.

All persons subject to this Policy must comply with its content irrespective of their position, function, form of engagement or the geographical location from which they carry out their activity.

4.3. Updates

This Policy shall be subject to periodic review in order to ensure that it remains appropriate to the applicable regulations, to the Organisation's organisational structure, to the recommendations of the competent authorities and to the needs arising from the effective functioning of the Internal Reporting System.

Amendments of a material nature must be approved by the competent governing body. Amendments of a merely organisational, operational or documentary nature that do not alter the essential principles of this Policy may be proposed by the Internal Reporting System Committee (CSII) for the corresponding approval by the Compliance Officer.

5. SCOPE

The purpose of this Policy is to establish the principles, guarantees and rules of operation of the Internal Reporting System of doValue and its subsidiaries, as well as to govern the protection of persons who report or publicly disclose information on infringements under the terms provided for in Law 2/2023.

The protection measures provided for in this Policy shall apply, as appropriate, to:

- Reporting Persons.
- Related Third Parties.
- The legal representatives of the employees when acting in an advisory and support capacity for the Reporting Person.
- Persons Concerned by the Report.

For the purposes of this Policy, those persons who meet the requirements and conditions provided for in Law 2/2023 and in the following sections of this Policy shall be considered Reporting Persons, Related Third Parties and Persons Concerned by the Report.

6. DEFINITIONS

For the purposes of this Policy, the following definitions shall apply:

- **Report**: Information submitted through the Internal Reporting System relating to facts, conduct or omissions that may constitute infringements falling within the scope of application of this Policy.
- **Internal Reporting System (SII)**: Integrated set of principles, procedures, resources, persons and channels made available by the Organisation for the receipt, management, investigation and monitoring of the reports made within the framework of this Policy.
- **Reporting Person**: Natural person who reports or publicly discloses information on infringements obtained in a work-related or professional context and who meets the conditions provided for in Law 2/2023. Reporting persons shall include, among others, employees, self-employed workers, shareholders, members of the administrative, management or supervisory body, persons working for or under the supervision of business partners, volunteers, interns, trainees and those whose employment or professional relationship has ended or has not yet begun.
- **Person concerned by the Report**: Natural or legal person to whom the facts, conduct or omissions described in a report received through the Internal Reporting System are attributed.
- **Related Third Parties**: Natural or legal persons connected with the Reporting Person who may suffer retaliation in a work-related or professional context as a consequence of a report, including, among others, co-workers, relatives, legal representatives of the employees or entities with which the Reporting Person maintains a significant professional relationship.
- **Head of the Internal Reporting System**: Body responsible for the supervision and functioning of the Internal Reporting System, appointed by the Board of Directors in accordance with Law 2/2023**.** At doValue, that function is performed by the Internal Reporting System Committee (CSII).
- **Internal Reporting System Committee** (CSII): Collegiate body appointed as Head of the Internal Reporting System, responsible for supervising the proper functioning of the System, ensuring compliance with this Policy and adopting the decisions necessary for its correct application.
- **System Delegate**: Member of the CSII appointed to perform the day-to-day management functions of the Internal Reporting System, including the receipt and processing of reports, the coordination of investigations, the maintenance of the corresponding records and the performance of the actions entrusted to them by the CSII.

- **Public disclosure**: Making information on infringements available to the public under the terms and conditions provided for in Law 2/2023.
- **Retaliation**: Any act or omission, threat or attempt thereof, prohibited by the applicable regulations, which causes or may cause unjustified detriment to a person as a consequence of having made a protected report or public disclosure.
- **Conflict of interest**: Situation in which a person's personal, professional or economic interests may compromise, or appear to compromise, their impartiality, independence or objectivity in the management or resolution of a report.
- **Good faith and reasonable grounds**: For the purposes of this Policy, a report shall be deemed to have been made legitimately where the reporting person has reasonable grounds to believe that the information reported is true at the time of its submission, irrespective of whether the facts may subsequently be substantiated or not.

7. HEAD OF DOVALUE'S INTERNAL REPORTING SYSTEM

The appointment of a Head of the System responds to the obligation established in Article 8 of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption.

The Board of Directors of doValue Spain Servicing, S.A.U. has appointed as Head of the Internal Reporting System the **Internal Reporting System Committee (CSII),** a collegiate body which acts with autonomy and independence in the exercise of its functions and which has the necessary competence, integrity, authority and resources to ensure the proper functioning of the Internal Reporting System.

The CSII is the body responsible for the general supervision of the Internal Reporting System, for monitoring its functioning and for adopting the decisions necessary to ensure compliance with this Policy and with the applicable regulations.

The composition of the CSII shall be as follows:

- Director of Legal Affairs and Data Protection Officer
- Director of Control & ERM and Compliance Officer
- Claims Control Coordinator

- Director of Labour Relations
- Senior Health and Safety Specialist

In order to facilitate the day-to-day management of the Internal Reporting System, the CSII shall appoint from among its members a delegate, who shall be responsible for the operational management of the system, the receipt and processing of reports, the coordination of investigation activities and any other functions expressly entrusted to them by the Committee, without prejudice to the powers and responsibilities pertaining to the CSII itself as Head of the System.

Where a situation of conflict of interest, absence, vacancy or any other circumstance arises that could compromise the independence or impartiality of any of its members, that member must refrain from taking part in the management of, or the decision-making relating to, the report concerned, and it shall be for the remaining members of the Committee to adopt the measures necessary to ensure the proper processing of the file.

The appointment, removal and any change in the composition of the CSII or in the person to whom the management powers of the System are delegated shall be notified to the Independent Whistleblower Protection Authority (Autoridad Independiente de Protección del Informante, A.A.I.) under the terms and within the time limits established in the applicable regulations.

8. DOVALUE'S INTERNAL REPORTING SYSTEM AND EXTERNAL REPORTING CHANNELS

8.1. DOVALUE'S INTERNAL REPORTING SYSTEM.

8.1.1. PURPOSE OF THE INTERNAL REPORTING SYSTEM.

doValue has an Internal Reporting System comprising various channels made available for the receipt and management of reports relating to facts or conduct becoming known in a work-related or professional context

- The following conduct, among others, may be reported through the Internal Reporting System: Infringements of European Union law falling within the scope of application of Directive (EU) 2019/1937 and of Law 2/2023, of 20 February
- Serious or very serious criminal or administrative offences.

- Breaches of the Organisation's Code of Conduct.
- Breaches of internal regulations, procedures, corporate policies or any other irregular or fraudulent conduct or conduct contrary to the ethical and compliance principles of the Organisation.

The Internal Reporting System constitutes the preferred channel for reporting this type of conduct and its purpose is to facilitate its early detection, assessment and investigation and, where appropriate, the adoption of the corrective or disciplinary measures that may be appropriate.

Notwithstanding the foregoing, not all reports received through the Internal Reporting System will fall within the scope of protection provided for by Law 2/2023. In particular, reports relating exclusively to breaches of the Code of Conduct or of internal regulations that do not constitute infringements of European Union law or serious or very serious criminal or administrative offences shall be managed through the System but shall not automatically give rise to the protection measures specifically provided for in that Law.

Nevertheless, the Organisation shall in all cases guarantee the confidentiality of the information received, the protection of the personal data processed and the diligent and impartial management of reports, in accordance with the provisions of this Policy and of the applicable regulations.

The classification of a report as falling within or outside the scope of protection of Law 2/2023 shall be the responsibility of the Internal Reporting System Committee or of the person to whom it delegates the management of the System, in accordance with the applicable internal procedure.

8.1.2. ACCESS TO AND OPERATION OF THE INTERNAL REPORTING SYSTEM.

The Organisation has an Internal Reporting System comprising various channels made available for the receipt and management of reports relating to facts or conduct occurring in a work-related or professional context.

Reports may be submitted on a named or an anonymous basis, and the confidentiality of the identity of the reporting person, of the persons concerned by the report and of any related third party shall be guaranteed in all cases, as shall the protection of the personal data processed.

Reports may be made in writing, verbally or by requesting a face-to-face meeting, in accordance with the provisions of this Policy and of the Internal Reporting System Management Procedure.

The channels made available by the Organisation for the submission of reports are the following:

- **doValue:** www.dovalue.whistlelink.com
- **TEAM4:** https://team4.canalhelas.com/home

Where the report is submitted through the platforms made available for that purpose, the system may generate credentials or tracking mechanisms enabling the reporting person to check the status of the report and to respond to the requests for information addressed to them.

For matters relating to situations of workplace harassment, sexual harassment or cyberbullying, the Organisation has specific channels managed in accordance with the provisions of the Protocol for the Prevention of Workplace Harassment, Sexual Harassment and Cyberbullying. Those channels form part of the general control framework of the Organisation and shall be managed in accordance with the specific applicable procedure, without prejudice to the general supervision pertaining to the Internal Reporting System Committee (CSII).

Likewise, the reporting person may request the holding of a face-to-face meeting with the person delegated by the CSII or with any other member appointed by it. The meeting must be held within the legally established time limit, that is, within a maximum period of seven (7) days from the request, in accordance with Law 2/2023, and shall be documented by means of a recording, subject to the prior consent of the reporting person, or by means of a complete and accurate transcript of its content, which may be reviewed, corrected and approved by the reporting person themselves.

Where a report is received by any member of the CSII or by any person of the Organisation other than the person delegated to manage the System, it must be forwarded immediately and confidentially to that delegate, in order to ensure the proper follow-up of the procedure and the protection of the rights of reporting persons, persons concerned and related third parties.

All reports received shall be managed in accordance with the provisions of the Internal Reporting System Management Procedure, ensuring compliance with the obligations of confidentiality, data protection, independence, objectivity and absence of retaliation provided for in the applicable regulations and in this Policy.

Reports may be received through the main channels of the Internal Reporting System or through other corporate channels specifically made available for particular matters. In all cases, reports falling within the scope of application of this Policy shall be incorporated into the Internal Reporting System and managed in accordance with the Internal Reporting System Management Procedure

8.2. EXTERNAL REPORTING CHANNELS.

Without prejudice to the use of the Organisation's Internal Reporting System, Reporting Persons may report the infringements falling within the scope of application of Law 2/2023 directly to the Independent Whistleblower Protection Authority (A.A.I.) or to any other competent authorities or bodies that may be applicable in each case.

The Organisation shall make available to potential Reporting Persons up-to-date information on the external reporting channels made available by the competent authorities and shall facilitate access to them through the appropriate corporate means.

The following channels, among others, may be used:

- External channel of the Independent Whistleblower Protection Authority (A.A.I.).
  https://www.proteccioninformante.gob.es/canales-de-presentacion-de-informaciones
- External channels made available by the competent regional authorities.
  https://www.proteccioninformante.gob.es/informacion-sobre-otros-canales-externos-de-informacion

- External channels established by European Union bodies, institutions or authorities where applicable.

The use of the external reporting channels shall not require the prior use of the Organisation's Internal Reporting System.

9. PRINCIPLES OF THE INTERNAL REPORTING SYSTEM

This Policy has taken into account the most advanced standards in this area in order to affirm its commitment and willingness to apply the highest guarantees of protection for Reporting Persons, both from the point of view of the protection of their identity and of the absence of retaliation against them.

For this reason, the following Principles shall be observed in the operation of the Company's Internal Reporting System:

(i) **Principle of Independence:** autonomy and the avoidance of conflicts of interest are guaranteed in the operation of the Internal Reporting System, as well as in the various stages of management of the Report received, its analysis, investigation and resolution and, finally, in the potential application of the response or *corporate defense* mechanisms, always seeking to protect two fundamental principles:

- The Organisation's commitment to regulatory compliance.
- The best legitimate corporate interest of the entity as opposed to any other personal interest or the interest of a group or of any other third party.

(ii) **Principle of Zero Tolerance and Respect:** The Company has implemented the Internal Reporting System on the basis of its commitment to zero tolerance of conduct contrary to the ethical, compliance and crime-prevention principles that form part of its corporate Compliance commitment. To that end, in all the communications and decisions inherent in the operation of the Internal Reporting System, the figure of the reporting person or *whistleblower* shall be respected and protected, ensuring the absence of any retaliation, adverse consequence or detrimental conduct against them merely by reason of the reporting and submission of a report.

(iii) **Principle of Confidentiality:** in accordance with the provisions of Article 24 of Organic Law 3/2018 on the protection of personal data and the guarantee of digital rights, as well as with the criteria established in Law 2/2023, of 20 February.

With particular emphasis, the Company guarantees and safeguards confidentiality, especially as regards any data that may reveal the identity of the Person concerned by the report and also the content of the Reports themselves.

These guarantees apply not only to Reports in which the Reporting Person has chosen to be identified, but also to those in which the anonymous option has been chosen.

(iv) **Good faith, objectivity and integrity**: reciprocally to the requirement of good faith in the submission of Reports, the Organisation shall seek to obtain, through their analysis and investigation, a proper and objective understanding of their content.

All of the foregoing shall be pursued through the honest purpose of protecting the legal interests at stake in the decisions and acts that may be carried out within the Organisation, as well as in the analysis of the reports concerning their failure to comply with the ethical, regulatory and crime-prevention standards and obligations existing within the entity.

(v) Principle prohibiting retaliation / detrimental conduct against Reporting Persons and Related Third Parties: doValue and its subsidiaries prohibit the adoption of retaliation against any Reporting Person or Related Third Party, including threats of retaliation and attempted retaliation. This prohibition covers, in addition to retaliation in the strict sense, any adverse treatment or detrimental conduct related to the report. Should the Company become aware that retaliation is occurring or has occurred, the Organisation shall adopt the protection measures necessary to stop, address and remedy such a situation.

10. PROTECTION PARAMETERS

10.1. PERSONS ELIGIBLE FOR PROTECTION

The Company shall provide protection both to the Reporting Person acting in good faith and to Related Third Parties against any detriment they may suffer as a result of reporting possible infringements of which they have become aware, as well as to those persons who have made a public disclosure regarding one of the infringements falling within the scope of application of the Internal Reporting System.

Likewise, the Organisation shall extend protection, under the terms legally provided for in this case, to the Persons concerned by the Report.

However, and as set out above, persons who report infringements not covered by Law 2/2023, of 20 February, shall fall outside its scope of protection.

10.2. CONDITIONS OF PROTECTION

A **Reporting Person acting in good faith** is one who has reasonable grounds to believe that the information reported is true at the time of the Report, even where they do not provide conclusive evidence. The protection of the Reporting Person shall not lapse by reason of the report ultimately not proceeding or of the facts not being substantiated, provided that such reasonable grounds existed, and it is recognised irrespective of the channel used. Every protected person shall be entitled to the support measures provided for in Law 2/2023 (information, advice and assistance), and may not be required to waive those rights in advance.

The following are **expressly excluded** from the Internal Reporting System of the Company: the information contained in Reports that have previously been rejected by any other corporate reporting mechanism in which the Report containing precisely such information has already been specifically rejected, assessed or resolved, provided that no additional and new facts or evidence are provided.

Likewise, information whose facts do not fall within the scope of application of the Internal Reporting System of DOVALUE and its subsidiaries shall also be rejected.

10.3. PROTECTION MEASURES FOR THE REPORTING PERSON AND RELATED THIRD PARTIES

The Company is responsible for guaranteeing the protection of Reporting Persons and Related Third Parties, in accordance with Article 39 of Law 2/2023, of 20 February. The Head of the System has the function of ensuring that such protection measures are effectively implemented within the Organisation.

PROHIBITION OF RETALIATION OR DETRIMENTAL CONDUCT

Every member of DOVALUE is strictly prohibited from adopting retaliation against Reporting Persons acting in good faith, including threats of retaliation and attempted retaliation.

The term **retaliation** means any act or omission, as well as any adverse treatment or detrimental conduct, that is prohibited by law or that, directly or indirectly, entails unfavourable treatment placing the persons suffering it at a particular disadvantage as compared with another person in the work-related or professional context, by reason of their status as Reporting Persons or Related Third Parties, or for having made a public disclosure.

For the purposes of Article 36.2 of Law 2/2023, detrimental acts suffered by the Reporting Person within the two years following the report or disclosure shall be presumed to be retaliation, unless proven otherwise by DOVALUE and its subsidiaries. In any proceedings, it shall be for the Company to prove that the measure adopted was based on duly justified grounds unrelated to the report.

Attached as **Annex 2** is an illustrative, non-exhaustive list of actions or acts falling within the definition of retaliation.

If the Company becomes aware that retaliation is occurring or has occurred, it shall take reasonable measures to stop and address it. In this regard, the situation of the Reporting Person or of the Related Third Party shall be remedied so as to restore them to the position corresponding to that in which they would have been had they not suffered the retaliation or detrimental conduct. For example:

- Reinstating the person in the same or an equivalent position, with the same salary, responsibilities, employment status and reputation;
- Allowing equal access to promotion, training, opportunities, benefits and rights;
- Restoring the person to their previous commercial position in relation to the Organisation;
- Ending or withdrawing any internal conflict or dispute that may exist against the person (for example, the attitude or the treatment afforded);
- Apologising for any detriment suffered;
- Awarding compensation for damages.

CONFIDENTIALITY AND PROTECTION OF PERSONAL DATA

DOVALUE is obliged to preserve the identity of the Reporting Person and of Related Third Parties, as well as to guarantee the confidential processing of their data.

In this respect, the Internal Reporting System is designed, established and managed in a secure manner, so as to guarantee the confidentiality of the identity of the Reporting Person and of any third party mentioned in the Report, and of the actions carried out in its management and processing, as well as data protection, preventing access by unauthorised personnel.

The Company undertakes not to process personal data that are not necessary in order to ascertain the acts or omissions identified in the reports inappropriately submitted through the Internal Reporting System and that, moreover, lack the appropriate legal justification; in that case, such data shall be deleted.

Likewise, the Company undertakes to comply with the time limits established in the applicable regulations and in the *Corporate procedure for the management of the Internal Reporting System*. In particular, the personal data relating to the Reports and to the internal investigations shall be retained only for the period that is necessary and proportionate; once three (3) months have elapsed from the receipt of the Report without investigation activities having been initiated, they shall be deleted, unless the purpose of the retention is to provide evidence of the functioning of the System, in which case they shall be kept in anonymised form, and in no case may they be retained for a period exceeding ten (10) years.

10.4. PROTECTION MEASURES FOR PERSONS CONCERNED BY THE REPORT

In accordance with Article 39 of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, the main protection measures to be implemented in respect of the Persons concerned by the Report are the following:

- Right to the presumption of innocence: the persons concerned by the Report may never be penalised without the truth of the facts contained in the Report having first been verified.
- Right of defence: the persons involved are given the opportunity to provide an explanation of the situation reported, being summoned to an interview or asked for clarifications aimed at establishing the facts.
- Right of access to the file: the Person concerned by the Report must be informed of the acts or omissions attributed to them. The right of access to the file shall be limited by respect for the guarantees of confidentiality and protection of the identity of the Reporting Person enshrined in Article 31 of Law 2/2023. This information shall be provided within a reasonable period, under the terms set out in Article 9.2(f), so as to observe the "time and manner deemed appropriate" to safeguard the successful outcome of the investigation.
- Protection of their identity, guaranteeing the confidentiality of the facts and data of the procedure.
- Compliance with deadlines: compliance with the time limits established in the applicable regulations and in the *Corporate procedure for the management of the Internal Reporting System*. Those time limits are detailed in section 10.5 of this Policy.

The scope of these measures shall be limited by the specific features that, depending on each type of Report or on its subject matter, may be applicable under the legislation in force.

10.5. COMPLIANCE WITH DEADLINES

The Organisation shall manage the Reports received in compliance with the time limits established in the applicable regulations, in particular in Law 2/2023, and in the *Corporate procedure for the management of the Internal Reporting System*. The main time limits are the following:

- Acknowledgement of receipt: this shall be sent to the reporting person within a maximum period of seven (7) calendar days following the receipt of the Report, unless doing so could jeopardise the confidentiality of the report.
- Response and closure of the file: the response to the reporting person regarding the investigation activities and the closure of the file shall take place within a maximum period of three (3) months from the receipt of the Report or, where no acknowledgement of receipt has been sent, from the expiry of the period of seven (7) calendar days following its submission. Where appropriate, the Person concerned by the Report shall also be informed of the closure, respecting at all times the obligations of confidentiality and protection of personal data.
- Extension: in cases of particular complexity requiring an extension, the period may be extended by up to a maximum of three (3) additional months. The extension shall be reasoned, shall be documented in the file and shall be notified to the reporting person.

The foregoing is without prejudice to the time limit provided for the holding of the face-to-face meeting, set out in section 8.1.2, and to the retention and deletion periods for personal data, set out in section 10.3.

10.6. ACTIVATION OF PROTECTION

The protection measures for the Reporting Person, Related Third Parties and Persons concerned by the Report shall be activated and shall commence as soon as the Report is received, and shall continue during and even after –

where necessary – the conclusion of the investigation or management process relating to the Report.

11. CONSEQUENCES OF NON-COMPLIANCE

All persons covered by this document are obliged to comply with its content. Where a breach thereof is identified, it may and must be brought to the attention of the Head of the System through its Internal Reporting System.

Where a contravention of the provisions of these texts is confirmed, the corresponding measures shall be adopted, including disciplinary measures (in the employment context) or contractual measures (in commercial relationships with Third Parties) deemed proportionate to the risk or to the damage caused.

The measures adopted from an employment perspective shall comply with the applicable regulations and shall be consistent, depending on the nature and seriousness of the facts, with the internal disciplinary regime, with the applicable Collective Bargaining Agreement and, failing that, with the Workers' Statute, without thereby losing firmness or proportionality in relation to the conduct committed. Where appropriate, the Legal Representatives of the Employees shall also be informed.

12. TRAINING

doValue shall ensure that all persons falling within the personal scope of the Internal Reporting System receive appropriate training on its existence and functioning.

Such training shall include, at least: the means of access to the channel and the infringements that may be reported, the guarantees of confidentiality and of protection against retaliation enjoyed by the Reporting Person, the possibility of making anonymous reports, the existence of external reporting channels (Independent Whistleblower Protection Authority, A.A.I.), the duty of confidentiality and the classification of its breach as a very serious infringement under Law 2/2023, the obligation to forward immediately to any of the members of the CSII any report received by means other than the channel, preserving confidentiality, and the consequences of the submission of reports that are shown to be false or to have been made in bad faith.

Training activities shall be delivered periodically and shall be updated whenever regulatory changes or significant modifications to the System occur. Documentary evidence shall be kept of all the training activities carried out.

13. PUBLICATION

This Policy is delivered to and made available to all Members of the Organisation, Business Partners and Third Parties through its publication on the Organisation's website, in a separate and easily identifiable section of the home page:

https://dovalue.es/

https://team4collection.com/

It is also published on the intranet of DOVALUE's intranet: www.doconnect.dovalue.it

The Company undertakes to disseminate and bring to the attention of all Members of the Organisation the information necessary to understand the Organisation's Internal Reporting System, its principles, guarantees and obligations, as well as its preventive purpose.

ANNEXES

ANNEX 1. Template for Submitting a Report

REPORT OF A REGULATORY INFRINGEMENT

Name of the Reporting Person (or, where applicable, “Anonymous”):

Area or Department (where identification is desired):

Person concerned by the Report (or reported person):

Date on which the facts were committed:

Facts:

Evidence provided with the Report:

Any witnesses to the facts:

Signature of the Reporting Person and date:

ANNEX 2. Non-exhaustive list of conduct considered retaliation.

- Dismissal, suspension, removal or equivalent measures relating to the employment contract, of a disciplinary nature or affecting professional career;
- Early termination or cancellation of contracts for goods or services;
- Non-renewal or early termination of a temporary employment contract;
- Change of job position or of duties, change of workplace location, salary reduction or change of working hours or of other working conditions;
- Demotion or withholding of promotion;
- Negative assessment or references regarding work or professional performance;
- Imposition of any disciplinary measure, reprimand or other sanction, including financial penalties;
- Denial of services;
- Denial of training;
- Harm, including to reputation, in particular on social media, or financial losses, including loss of business and of income;
- Any type of act, whether intentional or negligent, causing physical or psychological harm;
- Medical or psychiatric referrals;
- Negative assessment or references regarding their work performance;
- Coercion, intimidation, harassment or ostracism or isolation;
- Discrimination, or unfavourable or unfair treatment;
- Blacklisting on the basis of a sector-wide, informal or formal agreement, which may entail that the person will not find employment in that sector in the future;
- Disclosure of the identity of the Reporting Person;

- Financial loss;
- Cancellation or refusal of a licence or permit.