1. WELCOME TO DOGA'S INTERNAL CHANNEL

What is DOGA's internal channel and how to access it?

As part of its Internal Information System, the DOGA Group ("DOGA") provides all employees of DOGA, S.A. and ELECTRONIC MOVEMENT GROUP, as well as any third party linked to the organization or company ("Informant/s"), with the Internal Information Channel tool available in the "Submit a report" section. Through this channel, any indication or reasonable suspicion of the commission of criminal offenses and/or serious or very serious administrative violations that may have occurred can be reported confidentially.

"Communication" shall be understood as any verbal or written report made by the Informant regarding violations.

Can communications be submitted anonymously?

You can submit your communication anonymously by checking the anonymity box when submitting it, or even verbally through an audio recording.

In any case, the communication must contain sufficient information necessary for a proper understanding of the reported facts.

What are its principles?

The channel enabled by DOGA offers a series of guarantees, including the confidentiality and protection of the informant's identity, the possibility of submitting anonymous communications, and the prohibition of retaliation, which you can consult in the "Principles and Guarantees" section.

Once submitted, how will my communication be processed?

You can learn more about how the procedure for handling submitted communications works by accessing the "Communication Management Process" section.

To track your reported communications, you must go to the "Communication Follow-up" section.

How will my personal data be processed?

The use of DOGA's Internal Information Channel, as well as the information and documentation you send us, may involve the provision of personal data.

You can find information about how we process the personal data collected through the internal channel in the "Data Protection Information" section.

Are there other independent channels besides those provided by DOGA for submitting communications?

You are also informed that you have the option to submit your communication directly to various Independent Whistleblower Protection Authorities through external reporting channels. In the case of Catalonia, the competent body is the Anti-Fraud Office of Catalonia.

We remind you that DOGA's internal channel is not the appropriate means for requesting information or submitting complaints and/or claims. Specific channels have been enabled for these purposes, and they remain unchanged following the implementation of this channel.

2. GENERAL PRINCIPLES AND GUARANTEES OF THE SYSTEM AND THE INTERNAL CHANNEL

To submit communications and manage the information, DOGA has enabled the Internal Information Channel, which operates based on the following principles and guarantees:

2.1 Truthfulness and good faith

Communications submitted to DOGA's internal channel must adhere to principles of truthfulness and good faith. In any case, they must be based on reasonable suspicions or indications that may suggest the occurrence of behavior or conduct constituting a criminal offense or a serious or very serious administrative violation, or any actions or omissions that may constitute breaches of European Union law within DOGA.

It will be presumed, unless proven otherwise, that the information provided has been submitted by the informant in good faith. Regardless of this, DOGA will not accept communications that lack foundation, have been manipulated, are clearly false, or show evident bad faith.

2.2 Independence and autonomy

To ensure compliance with these principles, DOGA has appointed a System Manager who, in performing their duties independently and autonomously from the rest of DOGA's bodies, will oversee the proper functioning of the internal system and the Internal Information Channel.

To reinforce the independence, objectivity, and autonomy of DOGA's internal system, a technology provider has been engaged to outsource the solution that supports the Internal Information Channel. Our provider offers adequate and sufficient guarantees to ensure the security of personal data, the confidentiality of information, the independence of the system, and the secrecy of communications.

2.3 Confidentiality

DOGA's Internal Information Channel is designed, established, and managed securely, ensuring the complete and absolute confidentiality of the identity of the informant, any third party mentioned in the communication, as well as all actions carried out during its handling and processing.

To ensure the confidentiality of the internal system, DOGA has restricted access to the internal channel tool so that only the following individuals can access the personal data contained therein:

- System Manager
- Human Resources Manager, only when disciplinary measures against an employee may be applicable
- Head of the Legal Services Department, if legal action related to the facts reported in the communication may be necessary
- Whistleblower Software Apps, acting as the data processor
- Data Protection Officer

2.4 Anonymity

To ensure that you submit your information anonymously, you must check the anonymity box at the time of submitting your communication.

To ensure that communications are submitted and processed anonymously, the tool enabled by DOGA includes the following features:

- No cookies are tracked, and no IP addresses or IDs are stored, ensuring the informant's anonymity
- Metadata from all files uploaded to the channel is automatically removed
- To guarantee anonymity in cases where the informant chooses to report an incident verbally, the system can automatically distort the informant's voice

2.5 Reservation of the identity of the informant and affected individuals

The identity of the informant will remain confidential throughout all stages of the communication's handling and processing. Specifically, it will not be disclosed to third parties, to the person being reported, or to management personnel.

DOGA may only disclose the identity of the informant to the judicial authority, the Public Prosecutor's Office, or the competent administrative authority within the framework of a criminal, disciplinary, or sanctioning investigation resulting from the inquiry carried out.

La revelación de la identidad de la persona Informante fuera del supuesto permitido o la realización de indagaciones dirigidas a conocer datos de las comunicaciones presentadas, con independencia del cargo y funciones, supondrá la imposición de las medidas disciplinarias oportunas, en su caso.

2.6 Prohibition of Retaliation and Protection of the Informant

DOGA rechaza y no va a tolerar ningún tipo de represalia, en cualquiera de sus formas, incluidas las amenazas y las tentativas de represalias, contra las personas Informantes que presenten comunicaciones de buena fe a través del canal habilitado por DOGA.

The disclosure of the informant's identity outside the permitted circumstances, or any inquiries aimed at uncovering details of the submitted communications—regardless of position or role—will result in the imposition of appropriate disciplinary measures, if applicable.

Protection measures also apply to individuals who assist the informant in the process; those who are connected to the informant and may suffer retaliation; and legal entities for which the informant works, maintains another type of professional relationship, or holds a significant interest. This specifically includes legal representatives of employees, coworkers, or family members of the informant.

Anyone who believes they are being or have been subjected to any form of retaliation must report it immediately to mar.pedraza@doga.es.

To ensure compliance with this principle, all necessary disciplinary or liability measures will be taken to protect the informant. Among others, and by way of example, the following actions are considered retaliation:

(i) Any labor-related measure, whether individual or collective, that is judicially classified as unfair;

(ii) The termination of the employment contract, for any reason and regardless of whether it is temporary or permanent, that is judicially declared as unfair;
(iii) The non-renewal of a temporary contract despite the continued existence of the temporary needs that justified the hiring;
(iv) Any disciplinary measure that is judicially declared as unfair;
(v) Unjustified demotion or denial of promotions;
(vi) Unjustified cancellation of goods or services contracts;
(vii) Damages, including reputational harm, economic losses, coercion, intimidation, harassment, or ostracism;
(viii) Negative evaluations or references regarding professional or job performance;
(ix) Inclusion in blacklists or dissemination of information within a specific sector that hinders or prevents access to employment or the contracting of works or services;
(x) Denial of training opportunities;
(xi) Discrimination or unfavorable or unfair treatment.

Acts that constitute retaliation, as referred to in this section, shall be null and void by law and may give rise, where applicable, to disciplinary or liability measures, which may include compensation for damages to the affected person.

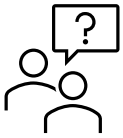
For the purposes of the protection measures covered in this section, individuals who have submitted reports that have been rejected by an internal reporting channel shall be excluded from such protection, or when:

- The reported facts lack credibility;
- The reported facts do not constitute a criminal offense and/or a serious or very serious administrative violation;
- The facts are clearly unfounded or there is reasonable evidence that they were obtained through the commission of a crime;
- The facts do not contain new and relevant information in relation to a previous report.

3. SUBMIT A COMMUNICATION

3.1. Who can submit a report?

Any person connected to DOGA who has obtained information or has a reasonable indication or suspicion of violations that have occurred or are very likely to occur within the scope of DOGA's activities, including:



- Any employee of DOGA, including shareholders, members of the management, administrative, or supervisory bodies, interns, volunteers, trainees, as well as former employees and individuals who had not yet started working but obtained the information during recruitment processes.
- All members of the management bodies of DOGA.
- Third parties not directly employed by DOGA, including clients, contractors, subcontractors, collaborators, and suppliers, provided that the report relates to potential irregularities connected to DOGA.

3.2. Through which channels can a report be submitted?

The system is available 24 hours a day, 365 days a year, from any device and in multiple languages, through the following access channels:

A form/platform available through DOGA's website, specifically in the Whistleblower Channel section located at the bottom of the Company's homepage, and in particular at the following link: https://whistleblowersoftware.com/secure/995c5c56-ebb8-4c1b-b32a-b3a5f3f1491d

The platform allows reports to be submitted via voice recordings.

At the request of the reporting person, through a meeting, within a maximum period of seven (7) days from the receipt of the request.

Likewise, all reports submitted verbally (including in-person meetings, phone calls, and voice messages) will be documented either through a recording or by means of a complete and accurate transcript of the conversation. In any case, the reporting person will be given the opportunity to review, correct, and approve the transcript of the conversation.

3.3. What types of situations should I report through the internal channel?

Reports submitted through the internal channel must relate to actions or omissions that violate current legal or internal regulations, or any other conduct that could be considered an administrative offense or a criminal act, known to have occurred within the scope of DOGA's activities. For example:

- Example 1. Use of invoices, import receipts, insurance documents, or shipping records with questionable authenticity as support for repeated transfers abroad.
- Example 2. Receiving numerous transfers or deposits for identical or repeated amounts without a justified reason.
- Example 3. Theft of company materials.
- Example 4. Physical assaults occurring on company premises.

Reports may also refer to any breach related to the Company's principles and values.

3.4. What information should I include when submitting my report?

The more detailed the information provided in the report, the easier it will be for DOGA to investigate. For example, your report may include the following information:

- Identification of the reporting person and their relationship with DOGA (this information is optional and not strictly necessary, as the report can be submitted anonymously);
- Individuals allegedly involved and their relationship with DOGA;
- Detailed description of the events and the location where they occurred;
- Approximate dates on which the reported events took place;
- If possible, supporting documents, witnesses, or any type of evidence—regardless of format—that can substantiate the reported facts.

3.5. What types of situations should not be reported through the internal channel?

- Reports not based on specific or concrete suspicions or indications (e.g., "I find person X's behavior suspicious; it makes me question their compliance with the code of ethics");
- Reports that clearly demonstrate bad faith (e.g., the same report submitted multiple times with different versions of the facts);
- Reports concerning facts that are entirely implausible (e.g., false or distorted reports);
- Reports about matters that do not constitute any violation that should be reported through DOGA's Internal Reporting Channel (e.g., a colleague's lack of hygiene or clothing choices);
- Reports with reasonable indications that the information was obtained unlawfully or through the commission of a crime (e.g., information obtained via hidden cameras or unauthorized recordings).

When any of these situations apply, before a report is deemed inadmissible for the reasons mentioned, the person responsible for managing DOGA's Internal Reporting System and Channel will inform the reporting person of the deficiencies in their submission and will grant them a period of five (5) business days to clarify, specify, or properly detail the facts in question. If the deficiencies are not corrected within the specified period, the report will be deemed inadmissible.

4. FOLLOW-UP OF SUBMITTED COMMUNICATIONS

When making the report, you may, if you wish, provide your full name, an address, email, or a secure location for the purpose of receiving notifications.

The main platform for submitting reports (via the Whistleblower channel available on the website) will generate a reference number and a personal, non-transferable password that will allow you to track the report and check its status.

Likewise, if an email address is provided, the system will automatically send updates regarding the status of the report.

5. PROCESS FOR HANDLING REPORTS

Once the report is submitted, it will be processed in accordance with the provisions outlined in the following sections:

5.1. Once submitted, how will my report be processed?

Once the report is received, the following steps will be taken:

5.1.1. Receipt of the report and acknowledgment of receipt

Once a report of a potential incident is received through DOGA's Internal Reporting Channel, the corresponding case will be initiated either by the Internal Reporting Channel Manager or by the designated external Manager. The case will be assigned a unique and differentiated reference number to ensure proper identification.

Upon receipt of the report, an acknowledgment of receipt will be sent to the whistleblower within a maximum of three working days, and under no circumstances later than seven calendar days from the date of receipt, unless such acknowledgment could compromise the confidentiality of the process. In the acknowledgment itself or afterwards, once the information has been reviewed, the Internal Channel Manager or the external Manager may, if deemed appropriate, request additional information to help clarify the reported facts more precisely.

All documentation collected in relation to the case must be stored in physical or electronic formats that are accessible only to individuals who need access to the information for processing purposes. It must be safeguarded with the level of security required by applicable legislation, particularly Law 2/2023 of February 20 on the protection of individuals who report regulatory violations and corruption, the General Data Protection Regulation (GDPR), and Organic Law 3/2018 of December 5 on the Protection of Personal Data and Guarantee of Digital Rights.

5.1.2. Review of the information received and preliminary report

The Internal Channel Manager or, where applicable, the external manager will prepare an initial preliminary report based on the data received. This report will include a detailed description of the facts, an analysis of the situation, and a legal assessment within a maximum period of ten working days from the acknowledgment of receipt of the report. If necessary, the document may include a proposal for urgent precautionary measures deemed appropriate for the specific situation. In any case, the confidentiality of the whistleblower will be guaranteed, and their identity, position at DOGA, or any other information that could lead to identification will be omitted.

Once all relevant information has been gathered, the Manager will carry out an assessment of the facts to determine whether they may constitute an incident or, conversely, whether they represent lawful conduct with no significant legal consequences (e.g., unverified rumors, isolated complaints about a supplier, etc.).

Based on the conclusion of this preliminary analysis, the Manager will issue a reasoned decision within a maximum of seven working days from the preparation of the report, choosing one of the following actions:

a) Accept the report and formally initiate the investigation process.

b) Reject the report and immediately close the case when any of the grounds for inadmissibility apply, or when the information received does not reveal a violation of the legal framework.

If the decision is to close the report, the whistleblower will be informed of this decision within a maximum of five working days from the date of the inadmissibility resolution. As soon as the report is deemed inadmissible, the whistleblower will be notified accordingly.

If the whistleblower disagrees with the decision, they will have the option to appeal to the competent administrative authority and/or pursue the matter through the appropriate judicial channels.

5.1.3. Strategy Selection

The Internal Reporting System Manager, in their role as investigator, will be responsible for defining the appropriate investigation strategy based on the circumstances of the case. If support from other departments is needed, the Manager may choose from the following alternatives:

a) Take full responsibility for designing, leading, and managing the investigation, with the option to occasionally seek assistance from other departments.

b) Outsource, under the Manager's control and supervision, those parts of the investigation process deemed necessary, depending on the level of need for external advice. This particular strategy is especially recommended in cases where the circumstances require exceptionally raising the confidentiality standards already in place in the procedure. In any case, the person responsible for conducting the investigation will remain the Internal Reporting System Manager.

5.1.4. Investigation Planning

The Internal Reporting System Manager will be responsible for planning the investigation, taking into account the nature and complexity of the case. If you'd like to share the rest of the section, I'll continue translating it for you.

The person in charge of the investigation must be guided by the following operational principles, although these are not intended to be exhaustive:

a) Identify the applicable legislation or regulations, as well as any business risks that may arise from the incident.

b) Identify relevant information whose review may be useful to the person in charge of the investigation.

c) Inform employee representatives, when applicable and necessary, of the need or urgency to adopt precautionary measures regarding the individuals under investigation. The implementation of such measures must follow criteria of timeliness and proportionality and remain in effect for the shortest time possible. These measures must be justified, unless their urgency requires immediate action, in which case the lack of justification must be subsequently addressed as soon as possible.

d) Prepare a script or plan for the investigation procedure, which should especially include the interviews to be conducted to clarify the facts, as well as the collection of other evidence deemed appropriate, with the support of the relevant departments. All actions must pay

special attention to workers' rights regarding privacy, data protection, and other legal safeguards.

e) Include in the investigation file any information of interest related to the employment history of the individual under investigation.

The investigation plan must minimize the impact of the process both on the organization and on the individuals under investigation.

5.1.5. Notification to the Affected Person

The Internal Reporting System Manager, in their role as investigator, must contact the individual to whom the reported facts are attributed, informing them of the following: their role as the person responsible for the investigation within the context of a potential incident, a summary of the alleged actions or omissions, and a general description of the main phases typically involved in the investigation process. Under no circumstances may the identity of the whistleblower be disclosed to the person under investigation.

As a general rule, this notification must be made within a maximum of ten working days from the formal acceptance of the report. However, if there are well-founded reasons indicating that such notification could compromise the proper development of the investigation, its delivery may be postponed. In such cases, the extension must be duly justified.

The method used to deliver this notification will be the one deemed most appropriate to ensure the effectiveness of the investigation, taking into account the specific circumstances of the case.

Once notified, the affected person may be heard at any point during the process.

At all times, the fundamental rights of the individual involved will be safeguarded, especially the right to the presumption of innocence and the protection of their reputation.

5.1.6. Conducting the Investigation

The person responsible for the investigation will carry out all actions deemed necessary to clarify the reported facts, identify potential responsible parties, and determine the corrective measures to be implemented. Among the main procedures that may be used are the following:

a) Maintain communication with the whistleblower to obtain additional information that may help expand or clarify the initial report.
b) Take statements or hear the version of events from the individuals involved.
c) Establish an evidentiary period during which both the whistleblower and the individuals under investigation may submit any documentation they consider relevant, as well as propose the appearance of witnesses to support their respective accounts. This period may not exceed seven working days.
d) Conduct interviews with witnesses to the reported events, ensuring at all times the same level of confidentiality required for the identity of the whistleblower.
e) Gather all documentation deemed relevant for a proper evaluation of the facts.
f) Implement surveillance measures, if necessary, provided they are absolutely essential to clarify the situation, comply with legal requirements, and adhere to the principles of reasonableness, suitability, and proportionality, while always ensuring the protection of the employee's privacy and the confidentiality of communications.
g) Carry out any other actions the investigator considers necessary to obtain a clear and complete understanding of the facts under review.

The maximum period for completing the investigation procedures will be three months from the date the report is received or, if applicable, from the end of the seven-calendar-day period established for issuing the acknowledgment of receipt to the whistleblower.

In cases that, due to their particular complexity, require an extension of the investigation period, this deadline may be extended for an additional period of up to three more months. Under no circumstances may the total duration of the investigation exceed six months.

5.1.7. Documentation of the Investigation Procedure

The investigation procedure must be fully documented in the corresponding case file, which will include both information related to the design and planning of the investigation, as well as supporting documents reflecting the results of the actions carried out by the investigator.

This documentation will be safeguarded with due diligence and will be inaccessible to anyone outside the investigation body.

5.1.8. Final Report

Once the investigation procedures are completed, the Manager must prepare a final report. This report must include, at a minimum, the following elements:

a) The nature of the incident investigated.
b) A detailed account of the verified facts and relevant findings.
c) A conclusive assessment of the facts, accompanied by one of the following decisions:

   i. Proceed with closing the case, either due to a lack of evidence supporting the reported facts, or because the verified facts are not considered significant enough to qualify as an incident.
   ii. Determine that a violation has occurred in accordance with the provisions of this procedure, and accordingly order the application of the corresponding disciplinary regime, as well as the imposition of appropriate sanctions based on the severity of the proven conduct.

The whistleblower will be informed of the conclusions, as well as the measures and actions taken, within a maximum period of one month from the date the report was received. This period may be extended when necessary due to specific circumstances of the case, particularly its nature and complexity, if they prevent a clear understanding of the facts. In any case, such an extension may not result in the process exceeding three months.

The Internal Reporting System Manager will report quarterly to the Board of Directors on the number of reports received, the topics and issues they address, the measures taken, and any other aspects that may contribute to strengthening the organization's reporting culture, integrity infrastructure, and adherence to the Company's principles and values. This reporting will always comply with confidentiality obligations regarding the information received.

5.2. Will I be informed of the outcome of the investigation? How?

Yes. The system will inform and update the status of the report at all times, and upon completion, it will send an email with the status of the report, a brief explanation of the conclusion reached, and the measures taken as a result of the investigation process.

6. DATA PROTECTION INFORMATION

In accordance with the provisions of Regulation (EU) 2016/679 of April 27, 2016, on the protection of natural persons with regard to the processing of personal data (hereinafter, the "GDPR"), and Organic Law 3/2018 of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter, the "LOPDGDD"), the following is hereby informed:

6.1. Identificacion of the Data Controller

The Board of Directors of DOGA, S.A. (hereinafter "DOGA"), with Tax Identification Number (NIF) A08299893, and registered address at A-2, Km. 583, 08630 Abrera, Barcelona, is the data controller responsible for the processing of personal data.

In any case, please note that DOGA has appointed a Data Protection Officer, whom you may contact at the following email address: dpd@doga.es.

6.2. Source of the personal data processed

The personal data collected and processed by DOGA may come from the following sources:

- Data provided by the informant when submitting a report through our internal reporting channel.
- Data that may be collected during the investigation of the reports.

6.3. Purpose of processing and legal basis

We will process your personal data solely for the purpose of confidentially recording, handling, managing, and investigating the reports submitted through DOGA's internal reporting channel.

This processing is based on DOGA's legal obligation in accordance with the provisions of Law 2/2023 of February 20, which regulates the protection of individuals who report regulatory breaches and the fight against corruption.

If the report contains special categories of personal data, and such data are relevant to the investigation, they will be processed based on substantial public interest (Article 9.2.g of the GDPR), as provided in Article 30.5 of Law 2/2023.

6.4. Recipients

Personal data concerning your identity may only be disclosed to the judicial authorities, the Public Prosecutor's Office, or the competent administrative authority within the framework of a criminal, disciplinary, or sanctioning investigation resulting from the inquiry carried out. Such disclosure is covered by a legal obligation applicable to DOGA.

Personal data may also be processed by DOGA's data processors, such as the technology provider supporting DOGA's Internal Reporting Channel, law firms engaged for legal advice if necessary, and group subsidiaries that may be affected by the report.

6.5. Data Retention

Your personal data will be retained only for the time strictly necessary to decide whether to initiate an investigation into the reported facts. In any case, if three months have passed since the receipt of the report without any investigative actions being initiated, the data must be deleted, unless the purpose of retention is to provide evidence of the system's operation.

Likewise, your personal data will be deleted in the following cases:

- When they are no longer necessary, especially if they involve special categories of data.
- When it is proven that the information provided, or part of it, is not truthful, from the moment this circumstance becomes known—unless the lack of truthfulness may constitute a criminal offense, in which case the information will be retained for the necessary duration of the judicial proceedings.

In cases where an investigation is initiated, the data will be retained until its conclusion. Afterwards, the data may be kept in a blocked state for the duration of the legal limitation periods applicable to actions related to this processing.

6.6. Exercising your rights

You may exercise the following rights:

- Right of access to your personal data to know which data are being processed and the processing operations carried out.
- Right to rectification of any inaccurate personal data.
- Right to erasure of your personal data, when applicable.
- Right to object to the processing, when applicable.
- Right to request the restriction of the processing of your personal data.

You may exercise your rights at any time and free of charge by sending an email to rgpd@doga.es, indicating the right you wish to exercise and your identifying information.

Please note that if an investigation is underway regarding the reported facts, or if judicial or extrajudicial actions are being carried out, the rights to erasure and objection may be limited if it is necessary to retain the identity of the informant to comply with a legal obligation.

Additionally, you are informed that you have the right to file a complaint with the Spanish Data Protection Agency (www.aepd.es) if you believe that a violation of data protection legislation has occurred in relation to the processing of your personal data.

6.7. Security

The Internal Reporting Channel platform includes the following technical security features:

- Certified compliance with ISO 27001:2013.
- Certified compliance with data protection regulations and information security measures under the data processing agreement, verified through an external audit in accordance with ISAE 3000 Type II.
- Regular external penetration testing.
- End-to-end encryption to ensure a high standard of data privacy in communications submitted through the Internal Channel.
- All data is strongly encrypted both in transit and during storage.
- Regular backups are performed to ensure data integrity, and these are stored in multiple locations to reduce the risk of data loss.

- Precise vulnerability scanning is carried out, and measures are implemented to ensure proper management.

6.8. Privacy Policy Uptates

This Privacy Policy may need to be updated, so it is important that you review it periodically.

Last updated: July 2025