ANNEX

TO THE

REGULATORY COMPLIANCE AND RISK PREVENTION **PLAN**

SOGRAPE GROUP

REGULATIONS

FOR THE WHISTEBLOWING CHANNEL

(Pursuant to the provisions of Law no. 93/2021 of 20 December, which establishes the general regime for the protection of whistleblowers, transposing into the internal legal order the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and Decree-Law no. 109-E/2021 of 9 December, which created the National Anti-Corruption Mechanism and established the General Regime for the Prevention of Corruption)

ARTICLE 1
SCOPE OF APPLICATION

1. The Sogrape Group, which includes the companies Sogrape SGPS, S.A., Grape Ideas - Turismo, Comércio e Serviços, S.A., Sogrape Distribuição, S.A. and Sogrape Vinhos, S.A., together referred to as the "Companies", has a whistleblowing channel, in strict compliance with the provisions of Law no. 93/2021 of 20 December, which establishes

the general regime for the protection of whistleblowers, transposing into the internal legal order the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019.

2. At the same time, the entry into force of Decree-Law no. 109-E/2021, of 9 December , which created the National Anti-Corruption Mechanism and established the General Regime for the Prevention of Corruption, determined in its Article 8(1) that the entities subject to that law should implement whistleblowing channels, aimed at reporting offences related to corruption, which, under the terms of Article 3 of the General Regime for the Prevention of Corruption, include the following crimes: corruption, undue receipt and offer of an advantage, embezzlement, economic participation in business, graft, abuse of power, prevarication, influence peddling, money laundering or fraud in obtaining or diverting a subsidy, grant or credit, as set out in the Penal Code, approved in the Annex to Decree-Law no. 48/95, of 15 March, in its current wording, in Law no. 34/87, of 16 July, in its current wording, in the Code of Military Justice, approved in annex to Law no. 100/2003, of 15 November, in Law no. 50/2007, of 31 August, in its current wording, in Law no. 20/2008, of 21 April, in its current wording, and in Decree-Law no. 28/84, of 20 January, in its current wording.

3. The purpose of these Regulations is to clarify the rules governing their operation for all members of statutory bodies and Employees who are part of the Sogrape Group's professional structure. They will apply regardless of the type of contractual relationship between each of the Companies and each of these members of statutory bodies and/or Employees, regardless of the position held, establishing the rules applicable to the internal whistleblowing channel, including the rules relating to the respective communication, as well as the procedures applicable to receiving,

processing and archiving incidents.

4. For the purposes of the previous paragraph, the Group's Regulatory Compliance Officer is responsible for managing the whistleblowing channel, including registering the communications received, processing them, investigating the respective cases and taking the final decision on whether to adopt the relevant measures or to close the case, as described below.

ARTICLE 2
GUIDING PRINCIPLES

1. The Sogrape Group has adopted procedures to ensure that the receipt, processing and filing of whistleblower reports are processed in an exhaustive, independent, autonomous, confidential and impartial manner, excluding from the investigation and decision-making process all persons who have a conflicting interest in the matter being reported.

2. All communications must be made in good faith, with adequate justification.

3. Deliberate, recurrent and unfounded use of the Whistleblowing Channel may constitute a disciplinary, civil or criminal offence.

4. The author of the report may, if they so wish, request anonymity by selecting this option on the Whistleblowing Channel questionnaire at the initial moment of reporting the irregularity.

5. Anonymity does not prevent the submission of documentation supporting the facts reported, which can be submitted in a field created for this purpose or independently.

6. Anonymity does not prevent the whistleblower from being contacted to obtain

information relevant to establishing the facts, and a documentary record of all interactions with the whistleblower must be kept confidential.

Article 3

SCOPE AND OBJECTIVE

1. For the purposes of these Regulations, the whistleblowing channel may report acts and omissions, whether wilful or negligent, attributable to members of statutory bodies, including non-executive members, employees, former employees, workers, former workers, volunteers and trainees, paid or unpaid, service providers, contractors, subcontractors and suppliers, as well as anyone who has taken part in recruitment processes within the Sogrape Group or in any negotiations that have not culminated in the conclusion of a contract, in the following areas:

    a) Public procurement;

    b) Financial services, products and markets and the prevention of money laundering and terrorist financing;

    c) Product safety and compliance;

    d) Transport safety;

    e) Environmental protection;

    f) Radiation protection and nuclear safety;

    g) Food and feed safety, animal health and animal welfare;

    h) Public health;

    i) Consumer defence;

j) Harassment and discrimination;

k) Working conditions;

l) Conflicts of interest;

m) Employee fraud;

n) Fraud by employees of organisations providing services to the Sogrape Group;

o) Theft or robbery and damage to property;

p) Breaches of confidentiality and data protection;

q) Failure to comply with European or national rules in the fields of:

    i) Public procurement;

    ii) Financial services, products and markets and the prevention of money laundering and terrorist financing;

    iii) Product safety and compliance;

    iv) Transport safety;

    v) Environmental protection;

    vi) Radiation protection and nuclear safety;

    vii) Food and feed safety, animal health and animal welfare;

    viii) Public health;

ix) Consumer defence;

x) Protection of privacy and personal data and security of the network and information systems;

r) The act or omission contrary to and detrimental to the financial interests of the European Union referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU), as specified in the applicable European Union measures;

s) The act or omission is contrary to the internal market rules referred to in Article 26(2) of the TFEU, including competition and state aid rules, as well as corporate tax rules;

t) The act or omission that contradicts the purpose of the rules or standards covered by any of the previous subparagraphs.

u) Violent, especially violent and highly organised crime, as well as the crimes provided for in Article 1(1) of Law no. 5/2002 of 11 January, which establishes measures to combat organised and economic-financial crime:

i) Drug trafficking;

ii) Terrorism, terrorist organisations, international terrorism and terrorist financing;

iii) Arms trafficking;

iv) Influence peddling;

v) Undue receipt of advantage;

vi) Active and passive corruption, including that practised in the public and private sectors and in international trade, as well as in sporting activity;

vii) Embezzlement;

viii) Economic participation in a business;

ix) Money laundering;

x) Conspiracy;

xi) Child pornography or procuring for prostitution or sexual act with minors;

xii) Damage to programs or other computer data and computer sabotage, as well as illegitimate access to a computer system;

xiii) Human trafficking;

xiv) Counterfeiting, the use and acquisition of counterfeit cards or other payment devices and their preparatory acts, the acquisition of cards or other payment devices obtained through computer crime, damage to computer programs or other data and computer sabotage, as well as illegitimate access to a computer system;

xv) Procuring for prostitution or sexual act;

xvi) Smuggling;

xvii) Trafficking and illegal modification of stolen vehicles.

v) Crimes of unduly offering an advantage, punishable under the terms of Article 372(2) of the Penal Code;

w) Crimes of fraud in obtaining a subsidy or grant, punishable under the terms of Article 36 of Decree-Law no. 28/84 of 20 January;

2. In addition to the provisions of Article 2(1) of Law no. 93/2021, of 20 December, the Sogrape Group's whistleblowing channel must be used to report, in particular: *(i)* harassment, in any of its forms; *(ii*) acts of discrimination/retaliation; (*iii*) non-compliance with rules or regulations; (*iv*) non-compliance with internal procedures and *(iv)* violation of the rules for preventing conflicts of interest.

Article 4

CONCEPT OF WHISTLEBLOWER

1. A whistleblower is anyone who reports or publicly discloses an offence on the basis of information obtained in the course of their professional activity, regardless of the nature of this activity and the sector in which it is carried out.

2. For the purposes of the previous paragraph, the following may be considered whistleblowers:

   a. Holders of shareholdings and members of Companies' statutory bodies, including non-executive members;

   b. Sogrape Group Employees;

   c. Service providers, contractors, subcontractors and suppliers, as well as any persons acting under their supervision and direction;

d. Volunteers and trainees, paid or unpaid.

3. The fact that the complaint or public disclosure of an offence is based on information obtained in the course of a professional, service provision or commercial relationship that has since ended, or during the recruitment process or other pre-contractual negotiation phase of an established or unestablished professional relationship, shall not prevent a person from being considered a whistleblower.

Article 5

DUTY TO REPORT

Members of statutory bodies of the Companies and Sogrape Group Employees have a duty to immediately report any alleged irregularity of which they are aware or which they can reasonably foresee being committed, regardless of the existence of supporting evidence or documentation.

Article 6

CONDITIONS FOR PROTECTING THE WHISTLEBLOWER

1. A Whistleblower who, in good faith and with serious grounds for believing that the information is, at the time of the report or public disclosure, true, reports or publicly discloses an offence or irregularity described in Article 3 of these Regulations shall benefit from protection and confidentiality under the terms of the following articles.

2. The protection afforded by these Regulations extends to (i) a person who assists the whistleblower in the whistleblowing procedure and whose assistance must be confidential, including trade union representatives or employee representatives; (ii) a third party who is linked to the whistleblower, such as a work colleague or family member, and who may be the target of retaliation in a professional context; and (iii)

legal persons or similar entities owned or controlled by the whistleblower, for whom the whistleblower works or with whom he or she is in any way linked in a professional context.

Article 7

CONFIDENTIALITY AND DATA PROTECTION

1. The Whistleblowing Channel guarantees the completeness, integrity and preservation of the complaint, the confidentiality of the identity of the whistleblower and their personal data, as well as that of the accused and third parties mentioned in the complaint, and the confidentiality of the communications received, which are restricted to the people responsible for receiving or following up on complaints.

2. The confidentiality obligation referred to in the previous paragraph extends to anyone who has received information about complaints, even if they are not responsible or incompetent for receiving and processing them.

3. Even if the whistleblower does not wish to remain anonymous, their identity will remain known only to the people responsible for receiving and following up on the complaint.

4. The confidentiality of communications will be ensured by all the people responsible for the operational management of the mechanisms and the procedures for receiving, processing and archiving these communications. Confidentiality will always be guaranteed, except in situations where the disclosure of information and/or the identity of those involved is required under the terms of the applicable legislation, within the scope of other investigations by competent authorities or subsequent legal proceedings, within the scope of which the Company is notified to provide such information.

5. The disclosure of information is preceded by written communication to the whistleblower stating the reasons for the disclosure of the confidential data in question, unless the provision of such information jeopardises related investigations or legal proceedings.

6. The confidentiality of the identity does not prevent the author of the report from being contacted, through the whistleblowing channel or by another written means made available for this purpose, with a view to obtaining information relevant to establishing the facts, keeping a documentary record of all interactions.

Article 8

PROHIBITION OF RETALIATION AND GUARANTEES FOR MEMBERS OF STATUTORY BODIES AND EMPLOYEES

1. Under the terms of Law no. 93/2021, of 20 December, it is forbidden to carry out acts of retaliation against the whistleblower.

2. An act of retaliation is any act or omission which, directly or indirectly, and even in the form of a threat or mere attempt, occurs in the professional context and is motivated by an internal or external complaint or public disclosure, and which is capable of causing the whistleblower unjustified damage to their property or non-pecuniary interests.

3. The following acts are presumed to have been motivated by an internal or external complaint or public disclosure, until proven otherwise, when carried out within two years of the complaint or public disclosure of the facts:

    a) Changes to working conditions or the provision of services, such as changes to duties, working hours, place of work or remuneration, failure to promote the Employee or failure to comply with labour duties imposed on the Company;

b) Suspension of an employment or service contract;

c) Negative performance appraisal or negative reference for the purposes of new job placement;

d) Non-conversion of a fixed-term labour contract into an open-ended contract, whenever the worker had legitimate expectations of such conversion;

e) Non-renewal of a fixed-term employment contract;

f) Dismissal;

g) Inclusion on a list, based on a sector-wide agreement, which could lead to the whistleblower being unable to find a job in the sector or industry concerned in the future;

h) Termination of contracts with third parties.

4. Threats and attempts at the acts and omissions referred to in the previous paragraph are also considered acts of retaliation.

5. The disciplinary sanction applied to the whistleblower up to two years after the complaint or public disclosure is presumed to be abusive.

6. Anyone who commits an act of retaliation shall compensate the whistleblower for the damage caused.

7. Irrespective of any civil liability, the whistleblower may request the appropriate legal measures to prevent or stop acts of retaliation.

8. Whistleblowers are generally entitled to legal protection under the terms of Law 34/2004 of 29 July.

9. Whistleblowers can benefit, in general terms, from measures for the protection of witnesses in criminal proceedings, provided for in Law 93/99 of 14 July.

10. Without prejudice to the provisions of the preceding paragraphs, the conduct of those who report evidence of irregular practices with manifest falsehood or bad faith, as well as those who breach the duty of confidentiality, shall constitute an offence that may be subject to disciplinary action that is appropriate and proportional to the offence, without prejudice to the civil and/or criminal liability that may arise for the perpetrator of said conduct.

Article 9

THE WHISTLEBLOWER'S RESPONSIBILITY

1. The reporting or public disclosure of an offence, made in accordance with the requirements imposed by this law, does not in itself constitute grounds for disciplinary, civil, misdemeanour or criminal liability for the whistleblower, except in cases where obtaining or accessing the information constitutes a crime.

2. A whistleblower who reports or publicly discloses an offence in accordance with the requirements imposed by this law is not liable for the violation of any restrictions on the communication or disclosure of information contained in the report or public disclosure.

3. The provisions of the previous paragraphs are without prejudice to the possible liability of whistleblowers for acts or omissions that are not related to the complaint or public disclosure, or that are not necessary for the complaint or public disclosure

of an offence under the terms of these Regulations and Law no. 93/2021, of 20 December.

Article 10

RECEIVING, REGISTERING AND PROCESSING COMPLAINTS

1. Irregularities can be reported:

   a) In writing, addressed to the whistleblowing channel manager, with the following contact details:

   b) Through the "*Whistleblowing Channel*", available on the Sogrape Group website (https://www.sogrape.pt);

2. The whistleblower must give as exhaustive a description as possible, but preferably objective, of the facts supporting the irregularity(ies) reported.

3. The communication will be received, analysed and will follow the processing flow defined in the approved process.

4. The whistleblower can attach documentation to this communication that supports the facts reported.

5. The Whistleblowing Channel, for the purpose of receiving complaints, is managed by an external and independent organisation.

6. Any report of wrongdoing can be submitted in writing, verbally or at a meeting, and anyone who receives a report of wrongdoing, provided it is covered by the Regulations, must alert the author to the existence of the Whistleblowing Channel, without prejudice to taking the initiative to report it immediately via the Whistleblowing Channel, in order to centralise all occurrences so that they follow the

same flow and benefit from equal treatment.

7. If, through the Whistleblowing Channel, the whistleblower requests to present their complaint at a face-to-face meeting, the Whistleblowing Channel manager must register the verbal complaint in one of the following ways:

    a. By recording the communication on a durable and retrievable medium;

    b. Through a complete and accurate written transcript of the communication, made by the person responsible for handling the complaint.

8. In the latter case, the whistleblower must be given the opportunity to verify, rectify and confirm the complaint by signing it.

9. The whistleblower should primarily use the Sogrape Group's whistleblowing channel and may only use other communication channels when:

    a. The person is not considered a whistleblower for the purposes of Article 4 of these Regulations;

    b. The whistleblower has reasonable grounds to believe that the breach cannot be recognised or resolved internally or that there is a risk of retaliation;

    c. The whistleblower lodges an internal complaint and is not informed of the measures subsequently taken within the time limits laid down by law; or

    d. The offence constitutes a criminal offence or an administrative offence punishable by a fine of more than €50,000.

Article 11
PROCESSING OF COMPLAINTS

1. Once the report has been received, it will be screened to determine whether it is within the scope and/or relevant to proceed to the investigation phase. All communications of potential or actual irregularities reported through the Whistleblowing Channel, in writing or in person, will be analysed. This analysis will give rise to a specific procedure, which may or may not lead to the opening of an investigation.

2. Whistleblowers will receive an acknowledgement of receipt and may be asked for additional information directly through the Whistleblowing Channel, while remaining anonymous if they so request.

3. If, following the preliminary analysis referred to in paragraph 1 of this article, it is concluded that the facts complained of relate to the matters and offences referred to in Article 3 of these Regulations, an investigation will be opened.

4. The whistleblower will be notified within seven days of the complaint and informed, in a clear and accessible manner, of the requirements, competent authorities and form and admissibility of the external complaint, under the terms of Article 7(2) and Articles 12 and 14 of Law 93/2021 of 20 December.

5. No later than 3 months after receipt of the complaint, the Group's Regulatory Compliance Officer shall notify the complainant of the measures planned or taken to follow up on the complaint and the reasons for these measures.

6. The whistleblower may request at any time that the Group's Regulatory Compliance Officer communicate the result of the analysis carried out on the complaint within 15

days of its conclusion.

7. The process for dealing with irregularities will be different depending on whether they concern harassment and discrimination or something else. The Sogrape Group's Human Resources Department is responsible for handling reports of irregularities relating to harassment and discrimination, as well as those relating to working conditions.

8. The handling of reports of other types of irregularities is the responsibility of the Group's Regulatory Compliance Officer.

9. The investigation may result in the need for communication or reporting to the competent authorities, which will be assessed in a reasoned opinion by the Group's Regulatory Compliance Officer and decided by the Board of Directors.

10. When the case is closed, the whistleblower will be informed.

11. All complaints will be analysed and investigation reports drawn up, and if the case does not proceed to the investigation stage, a reasoned report will be drawn up indicating the measures taken or the justification for not taking any measures.

12. Irregularities shall be communicated to the higher hierarchical level of the persons concerned by the complaint, if such transmission does not jeopardise the purposes of the procedure for reporting irregularities, and, where appropriate, to the competent authority.

13. A register will be kept for each case, which will include an indication of the measures adopted or the reasons for not adopting any measures. The results of investigations into irregularities are brought to the attention of the Management and Supervisory Bodies, always safeguarding the anonymity and confidentiality of the participant.

Article 12

KEEPING RECORDS AND DOCUMENTS

1. The Group's Regulatory Compliance Officer shall ensure that the records and the respective information are treated and safeguarded confidentially, and that the communications made, as well as the reports they give rise to under these Regulations, are kept on paper or on another durable medium that allows the full and unaltered reproduction of the information, for a period of five years and, regardless of this period, during the course of judicial or administrative proceedings relating to the complaint.

2. When the complaint concerns matters related to money laundering and terrorist financing, the communications made and the reports to which they give rise shall be kept for a period of seven years.

Article 13

PERSONAL DATA AND ITS STORAGE

1. The information communicated will be used exclusively for the purposes set out in these Regulations, in strict compliance with the provisions of the General Data Protection Regulation, Law no. 59/2019 of 8 August and other applicable legislation.

2. Supporting documentation and data collected during the preliminary analysis and investigation must be filed confidentially and securely. Security measures will be adopted for the storage of information in order to restrict access to authorised persons only.

3. As part of the activities carried out to investigate reported irregularities, the following categories of personal data may be collected relating to the complainants,

the person under investigation, witnesses or other individuals who are mentioned, such as:

a. Identification data: first name, surname;

b. Contact details: e-mail, address, telephone number;

c. Professional Data: Area/department, function;

d. Reported facts that could be part of suspicious activities;

e. Factual elements gathered in the investigation;

f. Information on private and family life;

g. Labour, economic and/or social relations;

h. Destination of the complaint;

i. Special categories of data.

4. Personal data that is not clearly relevant to dealing with a specific complaint will not be collected and, if collected by accident, will be deleted without undue delay.

5. The processing of personal data is legitimate whenever the following cases are applicable:

a. The legitimate interests pursued by the Sogrape Group to prevent and/or combat irregularities, in order to avoid damage (material and reputational damage), within the framework of transparency and compliance programmes;

b. Pursuit of legitimate interests in communicating the results of the investigation for the purposes of disciplinary action and/or appropriate complaint to the competent authorities. These grounds do not cover mandatory notifications made by the competent authorities in fulfilment of national and European legal obligations;

c. To fulfil a legal obligation;

d. Through consent;

e. For reasons of important public interest;

f. When criminal convictions and offences are involved.

6. The Sogrape Group may only disclose the identity of whistleblowers and/or reported persons to the competent authorities, as a result of a legal obligation or court decision, if the report gives rise to a criminal investigation or disciplinary action. Whenever necessary, and for the sole purpose of conducting investigations, the identity of whistleblowers and/or reported persons may also be disclosed to external investigators (such as lawyers) who are legally and/or contractually bound by secrecy and confidentiality obligations, in accordance with data protection principles.

7. In the event that the identity is disclosed for the aforementioned reason, the Group's Regulatory Compliance Officer will inform the whistleblower and the other persons concerned in advance, unless such information could jeopardise the investigation or legal proceedings. Similarly, when the competent authority informs the whistleblower that his or her identity will be revealed, that authority must justify the reasons for the disclosure.

8. Whenever necessary, relevant and legitimate for the purposes of these Regulations, data communications outside the European Union will respect the terms and

guarantees established in the General Data Protection Regulation regarding international data transfers.

9. To exercise their data protection rights (right of access, rectification, erasure, objection, restriction and portability), data subjects can send a written communication to the email address of the Privacy Ombudsman - privacy@sogrape.pt. In addition, data subjects have the right to lodge a complaint with the Supervisory Authority - the National Data Protection Commission.

10. As far as the right of access is concerned, at no time may third parties' personal information be disclosed to the data subject (such as the whistleblower, the person under investigation, witnesses or other individuals who are mentioned).

11. Supporting documentation and data collected during the preliminary analysis and investigation must be filed confidentially and securely. Technical and organisational security measures will be adopted for the storage of information, in order to restrict access to it to authorised persons only, as well as guaranteeing its integrity through access control and encryption.

Article 14
TERM

These Regulations come into force on 14 February 2024.

Control:

Approved by the Board of Directors of Guesi - Comércio e Serviços, S.A. on 14 February 2024