Glovo

For Internal Use Only

Ethics Channel Management Procedure

Version 3.0 - Valid from June 13, 2023

INDEX

1. Introduction

The aim of this Ethics Channel Management Procedure (the "**Procedure**") is to implement the operation of the Ethics Channel of GLOVOAPP23, S.A. and all the subsidiaries in its corporate group (hereinafter, jointly, the "**Company**" or "**Glovo**").

It establishes the procedure for handling queries and disclosures and for investigating disclosures, as well as, where appropriate, the sanctioning procedure for criminal acts or acts or omissions in breach of the applicable local Law, the law of the European Union, the Code of Ethics and other internal regulations It provides a description of the key elements - including human, organizational and documentary elements - used by Glovo to investigate and ascertain the scope of the allegations and handle queries relating to the Compliance Model.

Glovo is part of the Delivery Hero Group. Therefore, the content of this Procedure and the rest of the Compliance Policies and Procedures is in line with the policies, procedures and internal guidelines of the Group.

The procedure shall be applied by the HQ Compliance Officer and the Local Compliance Officer[1] of the country affected by the query or disclosure. On being notified of a possible breach, the HQ Compliance Officer must start the appropriate investigation, and the entire organization, the expert areas, the HQ Compliance Committee and the Regional Compliance Committees, if created, will assist the Officer in this endeavor. Everyone at every level of Glovo shall strive to ensure that this procedure is actually and effectively applied, and all parties involved must adhere to it.

[1] In those countries that do not yet have a designated Local Compliance Officer, references to such an Officer made in this Procedure shall be deemed to refer to the local professional who supports the HQ Compliance Officer in the handling of queries and disclosures.

In the event of any discrepancy between this Procedure (English version) and the various translations thereof, the English version shall prevail.

2. Scope of Application

Corporate Scope: This Procedure applies to the companies of the business group, including subsidiaries and affiliates over which Glovo has effective control or holds positions in the management bodies. However, the companies of the business group located in countries other than Spain may be governed by other specific rules if required by their applicable laws. The specific regulations applicable to each region shall form part of this Procedure by means of an appendix. Any conflict that may arise between this Procedure and the specific regulations shall be communicated to the HQ Compliance Officer and, if applicable, the most restrictive regulation or requirement will be applied. In case of doubt as to which standard applies, the local legislation shall prevail.

Personal Scope: This Procedure applies to all levels of Glovo, including management bodies, management positions, control bodies and the rest of Glovo's employees (hereinafter, "Glovo staff").

Relational Scope: This Procedure applies to any person who, in a professional or employment context, detects possible infringements (regardless of whether the professional or employment relationship has ended). This includes, among others, Glovo's suppliers, users of Glovo app (partners, clients and couriers), trainees, candidates, people who provide assistance to the reporting person, people around the reporting person who may suffer retaliation, as well as companies owned by the reporting person. If this is not possible, contracts shall be concluded only with companies that have similar policies or procedures.

Geographic Scope: This Procedure shall apply to any public and private relation Glovo establishes in any geographical area, both local and international.

3. Applicable Legislation

This Procedure complies with the following legislation:

- The Spanish Criminal Code (*Código Penal*)
- The Spanish Criminal Procedure Law (*Ley de Enjuiciamiento Criminal*)
- The Spanish Civil Procedure Law (*Ley de Enjuiciamiento Civil*)
- Regulation (EU) 679/2016 of 27 April 2016, the General Data Protection Regulation ("**GDPR**")
- Spanish Organic Law 3/2018 of 5 December 2018 on Data Protection and the Guarantee of Digital Rights ("**LOPD**")
- 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 (the "**Whistleblower Protection Directive**").
- Spanish Law 2/2023 of 20 February, on the protection of the whistleblowers reporting on legal infringements and corruption.
- Any other legislation in which Glovo operates, and it is required to comply with it.

This Procedure will be adapted to the legislative changes that take place in Spain and in the countries in which Glovo has activity of any kind, as well as to the criteria established in the judgments of the Supreme Court, Constitutional Court, Court of Justice of the European Union and the European Court of Human Rights and, in the same way, it will comply with the guidelines established in the guides, reports and resolutions of the national or European public administration.

Likewise, Glovo will comply with the local regulations that are applicable in the countries in which it operates. In this sense, the regulatory specificities applicable to each country or region will form part of this Procedure by means of an Annex. Any conflict that may arise between this Procedure and the specific regulations must be communicated to the HQ Compliance Officer and the provisions of the most restrictive regulation will be applied, where appropriate. In case of doubt about which rule to apply, the local legislation shall prevail.

4. General matters relating to making queries and disclosures

A) **Identification of preferred internal reporting channels**. Glovo makes an Ethics Channel to its employees and any third parties for making queries or reporting possible infractions. The Ethics Channel can be digitally accessed through the following preferred channels:

- The web form glovo.c-etico.es
- The email address compliance@glovoapp.com
- The DH Portal.

Communications sent through the Ethics Channel will be received by the HQ Compliance Officer, who will be responsible for the receipt of the report, and carrying out the appropriate investigations and deliberations, until he decides to either shelve the case or propose a sanction if the communications contain information on a

possible breach of the law, the Code of Ethics or any other applicable rule.

If the query or disclosure involves a foreign country, the HQ Compliance Officer shall forward it to the Local Compliance Officer, who will be collaborating in the appropriate investigations and deliberations until HQ Compliance Officer decides to either shelve the case or propose a sanction if the communications contain information on a possible breach of the law, the Code of Ethics or any other applicable rule.

Although communications will be sent to the HQ Compliance Officer, communications sent through Glovo's web form glovo.c-etico.es shall be initially received by a specialist external service provider in order to promote the use of the Ethics Channel and ensure the confidentiality of the process and, if applicable, the rights of the reporting person, the person concerned and other affected parties.

Communications addressed through the DH Portal are initially received by the DH Compliance Team. A notification is sent to the HQ Compliance Officer that is responsible for the investigation or shelving of the case.

The external provider (and DH in case of the DH Portal) shall inform the HQ Compliance Officer of all communications received through the web form in order for the said Officer to resolve the matters or queries raised or start the appropriate investigations and deliberations until they make the decision to either shelve the case or propose a sanction. If the case involves a foreign country where there is a Local Compliance Officer appointed, the decision shall not be made by the HQ Compliance Officer, and shall instead be forwarded by the HQ Compliance Officer to the relevant Local Compliance Officer in accordance with the local law, if applicable.

Glovo has an Ethics Channel at which two types of communications are received:

- **Queries:** regarding the Compliance Model and/or its internal regulations.
- **Disclosures:** on possible breaches of applicable local law, the law of the European Union, the Code of Ethics or its implementing regulations.

Both queries and disclosures can be sent through the web form, to the email address compliance@glovoapp.com, to the DH Portal.

If the person making the disclosure reports the information via a non-preferred channel, such as in writing to the sender's line manager, or by disclosing it to a member of the People department or the HQ Compliance Officer the person who receives the disclosure shall forward it to the HQ Compliance Officer, who must also submit it through the Ethics Channel.

Any Glovo employees who receive information about a disclosure made through the Ethics Channel or by any other method must observe the strictest confidentiality, refraining, among other things, from disclosing any information that might directly or indirectly reveal the identity of the reporting person, the person concerned or the affected parties and shall forward it to the HQ Compliance Officer or submit it through the Ethics Channel.

Anyone submitting a query must provide some contact details to which an answer can be sent.

Anyone making a disclosure has the option of giving their name or remaining anonymous, in which case it is recommended that they provide some contact details so that the allegations can be properly investigated more quickly and efficiently. Glovo shall also handle disclosures received by the External Provider in charge of managing the personal data in the Ethics Channel but under express instructions not to disclose such data to Glovo.

Communications shall include the following content, although certain sections are optional:

- **Queries**:

  1. Details or some contact details of the person sending the communication (required)
  2. The company to which the query relates (required)
  3. A description of the query (required)
  4. Evidence (optional)

- **Disclosures**:

  1. The reporting person's details (optional)
  2. The company to which the facts relate if known (required)
  3. Description of the facts (required)
  4. Evidence (optional)

Since any allegation (including unfounded rumours) can affect a person's reputation, and to enable it to carry out its investigations effectively, Glovo shall ask the reporting person, at any point of the investigation and as many times as needed, to provide all the information about the allegations in their possession, as well as any evidence they may have, although it is up to the reporting person whether or not to provide such information. It is worth noting that false accusations will not be tolerated and the reporting person may be sanctioned if the disclosure is deemed to have been made in bad faith based on reasonable indications that the allegations are not true, and the information provided is false, and reporting persons shall be subject to disciplinary and even legal action.

B) **External reporting channels**. In some countries, the Reporting person also have the possibility to communicate the information to reporting channels made available to the public by various authorities, such as:

- **European Anti-Fraud Office (OLAF)**

https://anti-fraud.ec.europa.eu/index_es

- Other local authorities (see relevant annex for more information).

5. Safeguards of the Ethics Channel and the Investigation Procedure

All queries and disclosures received through the Ethics Channel shall have the following safeguards:

i. **Security measures**: The Ethics Channel shall have appropriate technical and organizational security measures against the risk of dissemination, unavailability and loss or destruction of the information; i.e. measures to ensure the confidentiality, availability and integrity of the queries and disclosures received.

ii. **Confidentiality**: The confidentiality of the identity of the person making the communication, the reporting person and any third parties mentioned in the communication, as well as of the facts mentioned therein, shall be ensured, and the communication may only be accessed by personnel authorized for this purpose.

iii. **Privacy**: Personal data shall be processed as provided in the current applicable data protection legislation.

iv. **Diligent and reasoned answer**: Queries and disclosures shall be answered within the stipulated times and shall always be

sufficiently reasoned, responding to each of the issues raised.

Reporting persons shall have the following rights:

1. **Confidentiality**: The reporting person has the right not to have their identity revealed without their express consent (whether they provide their details or they don't provide them and their identity is subsequently discovered) to any person who is not authorized personnel, except pursuant to a necessary and proportionate obligation under the current law or as part of an investigation in connection with legal proceedings. In such case, the reporting person will be informed that their identity will be disclosed, unless such information could compromise the investigation or legal proceedings.

2. **Anonymity**: The reporting person may make the communication without revealing their identity.

3. **No retaliation**: The reporting person may never be subject to any retaliation of any kind for making a disclosure in good faith. They may only be sanctioned if the disclosure is deemed to have been made in bad faith on the basis of reasonable indications that the allegations are not true, and the information provided is false. The HQ Compliance Officer shall, together with the relevant departments, establish appropriate follow-up actions to ensure that this safeguard is complied with and, if required, implement measures for the protection of persons concerned.

Information: The reporting person shall receive an acknowledgement of receipt within a maximum of seven (7) days from receipt of the disclosure in the Ethics Channel. In addition, the reporting person shall receive, within three (3) months following date acknowledgment of the receipt of the disclosure by Glovo (or if no acknowledgement was sent to the reporting person, three (3) months from the expiry of the seven-day period after the report was made), containing information on the status of the disclosure and, if applicable, on the action that has been planned or adopted. This is without prejudice to the communication to be sent once the investigation has been completed.

The persons concerned shall have the following rights:

1. **Confidentiality**: The person concerned has the right not to have their identity revealed without their express consent to any person other than authorized personnel, except pursuant to a necessary and proportionate obligation under the current law or as part of an investigation in connection with legal proceedings.

2. Right to **honour** and **Presumption of Innocence**: The person concerned has the right to be presumed innocent and may therefore not be sanctioned or penalized until the investigation has been completed. Notwithstanding the foregoing, if it is found during the investigation that the person concerned is still engaging in a breach, interim measures may be taken, all this in accordance with the legislation in force from time to time and subject to the limitations envisaged therein.

3. **Right to make a statement and submit evidence**: The person concerned has the right to, make a statement in the investigation procedure or avail themselves of the right not to incriminate themselves. They shall also have the right to use any means of evidence

that they may deem appropriate for their defence (such as witnesses, documents, etc.). In any event, the person concerned must be given the opportunity in any investigation to make a statement and provide evidence before the end of the investigation. The person concerned can also be accompanied by an employees' representative or an attorney to make the statement, if requested in advance and provided that said representative or attorney is not involved in the facts under investigation. This circumstance shall be recorded in the minutes of the statement.

4. **Information**: The person concerned has the right to know that they are the subject of a disclosure and of the results of the investigation, access to the report and the information contained in the investigation file and any corrective measures that may be applicable, except for information that is expressly prohibited by law, such as the identity of the person making the disclosure.

   The person concerned shall be informed of the disclosure as soon as possible provided that this does not jeopardize the investigation. In this latter event, they shall be informed of the disclosure before they are summoned to make a statement. If the allegations are not true or accurate or do not constitute wrongdoing, the person concerned shall have the right to have this fact recorded. In such case, if the investigation into the person concerned was widely known about, the HQ Compliance Officer or the relevant Local Compliance Officer shall, on the request of the person concerned, may send an internal communication to everyone in that person's department or in any other departments that may be deemed appropriate, as applicable, stating that the investigation has been completed, and it has been concluded that the allegations were not true or accurate or did not constitute wrongdoing.

5. **Right to due process**: The person concerned has the right to due process in accordance with the law and the internal regulations applicable to the process, which shall include, in addition to the above and among others, adherence to the stipulated deadlines (without undue delay), the right to decision makers being objective and impartial (without a conflict of interest), and the right to any measures taken being proportionate to the seriousness of the facts in any event (proportionality of the sanction or penalty).

<u>The Ethics Channel must be designed and managed in accordance with the provisions of the current data protection legislation, and it must therefore comply with the following</u>:

i. The data contained in the Ethics Channel may be accessed solely by the Compliance Officer, and those internal or external persons who assist them in the management and processing of the communications received.

ii. The personal data contained in the Ethics Channel may only be retained for as long as necessary to decide on whether an investigation into the allegations should be started. In any event, such personal data must be deleted from the Ethics Channel three (3) months after it was entered. If the disclosure has not resulted in any action, the information shall be deleted, unless the purpose of the conservation is to leave evidence of Glovo's Compliance Model.

Communications that have not been followed up (not admitted for investigation) may only be kept in the Ethics Channel in anonymized form. Notwithstanding the foregoing, the processing of the personal data may continue for the purpose of investigating the allegations outside the Ethics Channel.

The personal data of the reports admitted for processing and the registry shall be kept outside the reception channel for the duration of the investigation and, in general, up to a maximum period of ten (10) years from the date of receipt of the report. However, the maximum retention period may be extended in some cases for example, to prove the effective functioning of our Compliance Model or when the reported event constitutes a criminal offense and the data must be retained during the corresponding legal proceedings.

iii. All irrelevant disclosures and disclosures whose allegations are found, following an investigation, not to be true or accurate or not to constitute any kind of wrongdoing shall be immediately shelved. This is without prejudice to the fact that the data and information shall be stored in the appropriate repository.

iv. Personal data that is not relevant for processing a disclosure shall not be collected, and any that is collected by accident must be deleted without undue delay.

v. In case the information received contained personal data considered special category of personal data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a person's sex life or sexual orientation), it shall be immediately deleted from the Ethic Channel, unless it proves necessary for conducting the investigation.

vi. The person concerned and the reporting person, as well as any third parties connected to the facts, shall be informed of the processing of personal data within a reasonable time, and in any event within a maximum of one (1) month from the date of receipt thereof at the Ethics Channel, unless this could jeopardize the investigation of the disclosure, in which case they must be informed after one (1) month but in any event before the date of completion of the investigation.

6. Encouraging the use of the Ethics Channel, and Rules of Use

Glovo shall conduct awareness campaigns on the use of the Ethics Channel on a regular basis for all employees, encouraging disclosures of any conducts that are contrary to law or ethics that they have identified or they believe they have identified.

If no communications are received at the Ethics Channel for six (6) months, the company shall verify that the Channel is in existence, that it is operating properly and that employees are aware of it. If it identifies a problem, this shall be immediately resolved (for example, by issuing an internal communication to all employees informing them of the safeguards provided by the Channel for all reporting persons).

The information or rules of use of the Ethics Channel shall include, among other matters:

1. Basic principles of the Ethics Channel and the investigation process
2. Who can use the Ethics Channel
3. What types of communication are accepted at the Ethics Channel
4. How to make a disclosure through the Ethics Channel
5. Response times
6. The rights and safeguards of the reporting person and the person concerned, including in particular:

    ★ The fact that there will be no retaliation against reporting persons acting in good faith. There must also be a warning about making false disclosures and the fact that doing so may constitute a breach.

    ★ The confidentiality of the reporting person's identity and of the investigations carried out.

7. Management of queries and disclosures received through the Ethics Channel

The following definitions shall apply to the process of handling queries and disclosures:

- **Querying Person**: A person who submits a query about Glovo's Compliance Model and/or Glovo's internal regulations.

- **Disclosure**: Any revelation of information that makes a breach or possible breach known.

- **Reporting Person**: A person who discloses or reveals information about any breaches identified by them.

- **Person Concerned**: A person accused of, or associated with, the alleged breach.

- **Breach**: Any conduct that is contrary to law, the Code of Ethics or Glovo's policies and procedures including, among others:

    - Committing a criminal offence, such as fraud, bribery or any other kind of corruption
    - Breach of a contractual and/or legal obligation
    - Mismanagement of a financial or other nature
    - Unethical conduct
    - Endangering any person's health and/or safety
    - Causing serious damage to the environment
    - Discriminating or creating a hostile work environment

- **Affected Person**: The person referred to in the disclosure.

- **Retaliation**: Any act or omission directly or indirectly caused by the reporting person's disclosure that causes or may cause unjustified harm to the reporting person in a work-related context. Examples include:

    - Dismissal or suspension
    - Demotion or refusal to promote
    - Refusal to provide training
    - Negative assessments at work, or giving bad references.
    - Disciplinary action
    - Harassment or intimidation
    - Discrimination or unfavourable treatment

- Non-renewal of a temporary contract, or non-conversion into a permanent contract
- Replacing the terms of employment or retirement with less favourable terms
- Reputational damage or blacklisting
- Posting the employee to a different place without justification, or refusing a transfer
- Refusing to give the employee an appointment in relation to a service or position

- **Channel Manager**: The third-party recipient of the communication that manages the Ethics Channel.

- **HQ Compliance Committee**: The body, chaired by the HQ Compliance Officer, with autonomous powers of initiative and control that is in charge of overseeing compliance with Glovo's Compliance Model.

- **Regional Compliance Committee**: A committee with control functions delegated by the HQ Compliance Committee can be appointed. If so, this Committee shall be responsible for assisting and supporting the HQ Compliance Committee.

- **Head of the Investigation**: The person or committee leading the investigation into the disclosure at the HQ Compliance Officer's request.

- **People Department**: The department in charge of assessing, proposing and, where applicable, imposing sanctions (in coordination with the HQ Compliance Committee) on employees who have committed a breach.

- **Board of Directors**: The highest body in the Company's control structure that must be informed of any very serious breaches and of breaches committed by a director or critical business partner.

Below is the procedure to be followed on receipt of a query or disclosure of breaches through the Ethics Channel:

i) Queries

1. Communication of the Query	Glovo makes the following communication channels available to anyone wishing to submit a query: • The web form glovo.c-etico.es • The email address compliance@glovoapp.com • Writing to the sender's line manager, a member of the People Department or the HQ Compliance Officer.
2. Assessment and Referral to the HQ Compliance Committee	**Queries through the Web Form**: If the query is received through the web form, the Channel's external manager shall send the query about the Compliance Model and/or its internal regulations to the HQ Compliance Officer for assessment. In addition, the manager shall also send, in the same communication as that containing the query, a brief analysis thereof with any suggested responses it may deem appropriate.

	Queries by e-mail: The Compliance team shall analyse the query and draw up any response it may deem appropriate. **Queries made directly to the HQ Compliance Officer:** The required information shall be assessed either by the HQ Compliance Officer or by the Compliance team.
3. Acknowledgement of Receipt and Recording	The querying party shall be given an acknowledgement of receipt in any event, and a record of queries accepted on the basis that they were deemed appropriate shall be kept.
4. Resolution of the Query	The HQ Compliance Officer will not answer queries that do not relate to the Compliance Model and/or its internal regulations, and shall instead take any of the following actions: • If, due to its type or subject matter, it pertains to another available channel or it falls within the remit of another area or department, the person who made the query shall be informed so they can send it to that area or department. • Pointless, trivial or unimportant communications shall be deleted, and the querying person will only be informed of this if they expressly ask in writing for an update regarding the status of their communication. A response shall be drawn up by either the HQ Compliance Officer / Local Compliance Officer of the foreign company to which the query relates or by the Compliance team and shall be sent to the querying person, and a record of the response given must be made and stored together with the query received. The querying person must also be informed when the query process is completed. The documents relating to the query shall be filed in the HQ Compliance Officer's folder created for this purpose and shall be retained for the amount of time stipulated in the data protection legislation.

ii) Disclosures

1. Early Detection - Responsibilities	Everyone at every level of Glovo is required to raise awareness of the company's zero tolerance policy to criminal risks and must therefore remain alert to any situation of risk that may be identified. For this reason, participation is encouraged, and everyone at every level is encouraged to disclose any irregularities of which they may become aware.
2. Making the Disclosure	Glovo makes the following communication channels available to anyone wishing to make a disclosure: • The web form glovo.c-etico.es • The email address compliance@glovoapp.com

	• The DH Portal. • Writing to the sender's line manager, a member of the People department or the HQ Compliance Officer. In such cases, the person who receives the disclosure shall forward it to the HQ Compliance Officer through the Ethics Channel. Any Glovo employees who receive information about a disclosure made through the Ethics Channel or by any other method must observe the strictest confidentiality, refraining, among other things, from revealing any information that may directly or indirectly reveal the identity of the reporting person, the person concerned or the affected parties. Any Glovo employee who receives a disclosure intended to be sent through the Ethics Channel must immediately forward it to the Compliance Team through the email address compliance@glovoapp.com and proceed to delete all the information in their devices, preserving the confidentiality of the case.
3. Assessment and Referral to the HQ Compliance Officer	When a disclosure is received through the web form or the DH Portal, the Channel's external manager shall assess its merits, send an answer acknowledging receipt, and forward it to the HQ Compliance Officer if necessary. In the said communication, the external manager must include a brief preliminary assessment of the disclosure, with their recommendation on whether it should be investigated or shelved. The obligation to forward the disclosure to the HQ Compliance Officer will not apply if the HQ Compliance Officer is the person concerned, in which case the Channel's external manager will forward it to another member of the Compliance Committee for them to deal with. In any event, the Channel's external manager may assist the HQ Compliance Committee in the investigation of the facts. The Channel's external manager must send an e-mail to the HQ Compliance Officer (or to another member of the HQ Compliance Committee if the HQ Compliance Officer is the person concerned) informing them of the disclosure received within no more than 72 hours of receipt.
4. Assessment and Classification	The HQ Compliance Officer shall carry out a preliminary analysis of the information received in order to check its truthfulness, clarity and comprehensiveness, as well as the relevance of the allegations. One of the following decisions shall then be made: - Accept the disclosure on the basis that the alleged facts involve a possible breach of the law, the Code of Ethics

	or Glovo's internal regulations. - Dismiss the disclosure on the basis that the claims of breach are unfounded or that no breach has taken place, in which case a brief report on the reasons for the dismissal must be drawn up. In this case, all documents and information will be deleted.
5. Acknowledgement of Receipt, Information on the Acceptance or Dismissal of the Disclosure, and Recording	On receipt of the disclosure, the reporting person shall be given an acknowledgement of receipt and shall subsequently be informed of whether the disclosure has been accepted or dismissed. Before responding to the disclosure or starting an investigation, the HQ Compliance Officer shall register the disclosure received in the restricted folder that must remain confidential. If the disclosure concerns the HQ Compliance Officer, the information must be placed in a different restricted folder that cannot be accessed by HQ Compliance Officer.
6. Additional Measures	The HQ Compliance Officer may take, or ask the appropriate department to take, any additional urgent measures that may be deemed necessary to ensure the effective investigation of the facts, as well as to ensure, where applicable, that there is no retaliation against the reporting person. In addition, the HQ Compliance Officer may also inform the relevant Local Compliance Officer, if appointed, of the start of the investigation if their collaboration is required due to the disclosure involving a foreign country. In any event, the HQ/Local Compliance Officer can ask the HQ Compliance Committee for advice and support throughout the investigation.
7. Investigation and Resolution	The Head of the Investigation will be the HQ Compliance Officer, and will have support from the Ethics Channel's external managers or other specialized people where appropriate. The aim of the investigation is to clarify the facts and identify responsibilities. A more detailed description can be found in the Investigation Procedure. The investigation shall end with the issue of a report setting out the facts, the evidence examined and the conclusion of the investigation, where appropriate including a proposal for the steps to be taken, which must be approved by the HQ Compliance Officer. If the wrongdoing to which the sanction relates may lead to the legal person being charged with a criminal offence, the Board of Directors must decide on the steps to be taken, taking into account the proposal made by the HQ Compliance Officer in the final report on the investigation.

8. Sanctioning Procedure	Common Provisions: The following aspects, among others, must be taken into account when imposing a sanction or penalty: 1. Any previous breaches, provided that the investigation process has been completed. 2. The time elapsed since the last sanction or penalty. 3. The seriousness of the facts investigated. 4. The amount of time during which the breach took place. 5. Whether the conduct was malicious or reckless. 6. The existence of mitigating circumstances, which shall be the following: o Confession. o Collaboration during the investigation. o Reparation or mitigation of the consequences of the damage. All steps taken shall be properly documented. If the infringement is minor, the People department or the relevant department must decide on the disciplinary action to be taken. In the case of serious and very serious infringements, on the other hand, the damage, possible improvements and channels for informing the authorities if the facts constitute a criminal offence must also be assessed. If the facts constitute a criminal offence, the HQ Compliance Officer shall inform the Board of Directors of the possibility/need of taking any legal action it may deem appropriate. Employees: If a breach is identified after completing the investigation and the person responsible for it is a Glovo employee, such person may be sanctioned in accordance with the provisions of the applicable Collective Bargaining or Sectorial Agreements or any equivalent provisions, applying Glovo's Disciplinary Procedure. Senior Officers, Directors, Members of the Board of Directors: If a breach is identified after completing the investigation and the person responsible for it is a senior officer, director or member of Glovo BoD, such person may be sanctioned in accordance with the current applicable legislation. Suppliers and other third parties: If a breach is identified after completing the investigation and the person responsible for it is a supplier of Glovo or

	another third party, the appropriate contractual measures shall be taken in accordance with the current applicable legislation.
9. Completion of the Investigation	If the final report following the completion of the investigation contains a proposal for a sanction or penalty or corrective measures, the HQ Compliance Officer must follow it up and attach the resulting documents to the report. Both the reporting person and the person concerned shall be informed in writing of the end of the procedure. The communication shall state at least whether any wrongdoing was identified in the allegations and, if so, the action that has been planned or taken. The person concerned shall also be informed if the allegations were untrue or inaccurate or did not constitute any kind of wrongdoing and, if the investigation was widely known about, about the possibility of sending an internal communication to everyone in that person's department or in any other departments that may be deemed appropriate, as applicable, stating that the investigation has been completed and has concluded that the allegations were not true and/or accurate or did not constitute wrongdoing. The documents relating to the investigation shall be filed in the confidential folder created for this purpose and shall be retained for the amount of time stipulated in the data protection legislation (see the "Investigation Procedure").

8. Updates and improvements

This Procedure shall be updated on a regular basis to reflect any changes to the Compliance Model.

Glovo shall constantly verify the application of this Procedure and shall propose appropriate amendments in the following circumstances:

1. In the event of a legislative change.
2. If it becomes apparent that relevant breaches of this Procedure have taken place.
3. If there are significant changes to Glovo or its activities.
4. In accordance with Delivery Hero instructions.

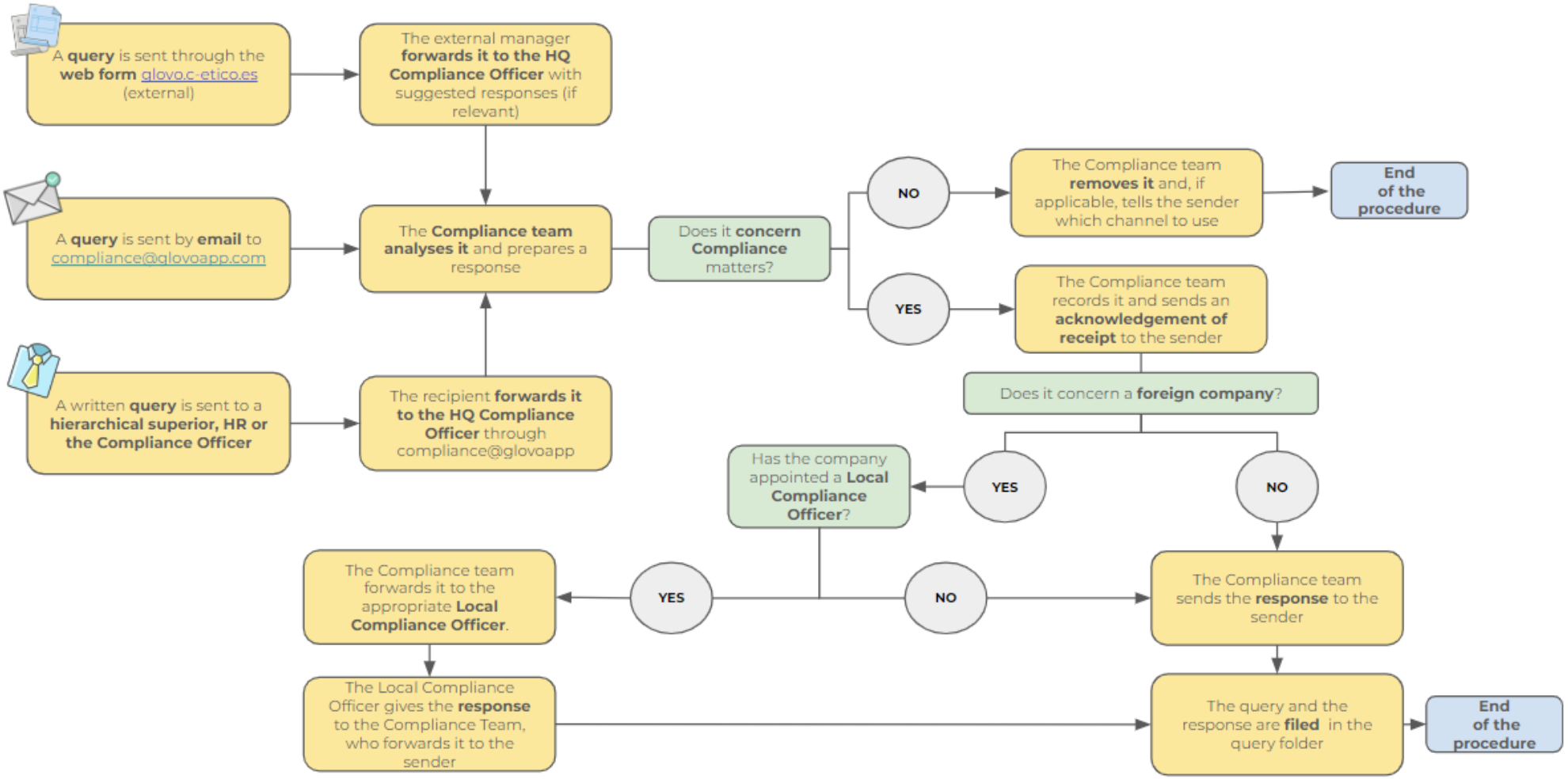
9. Approval and Revision Information

	Contact Details
Prepared by **Policy Owner**	GRC Team compliance@glovoapp.com
Verified by	Compliance Committee
Approved by	Board of Directors

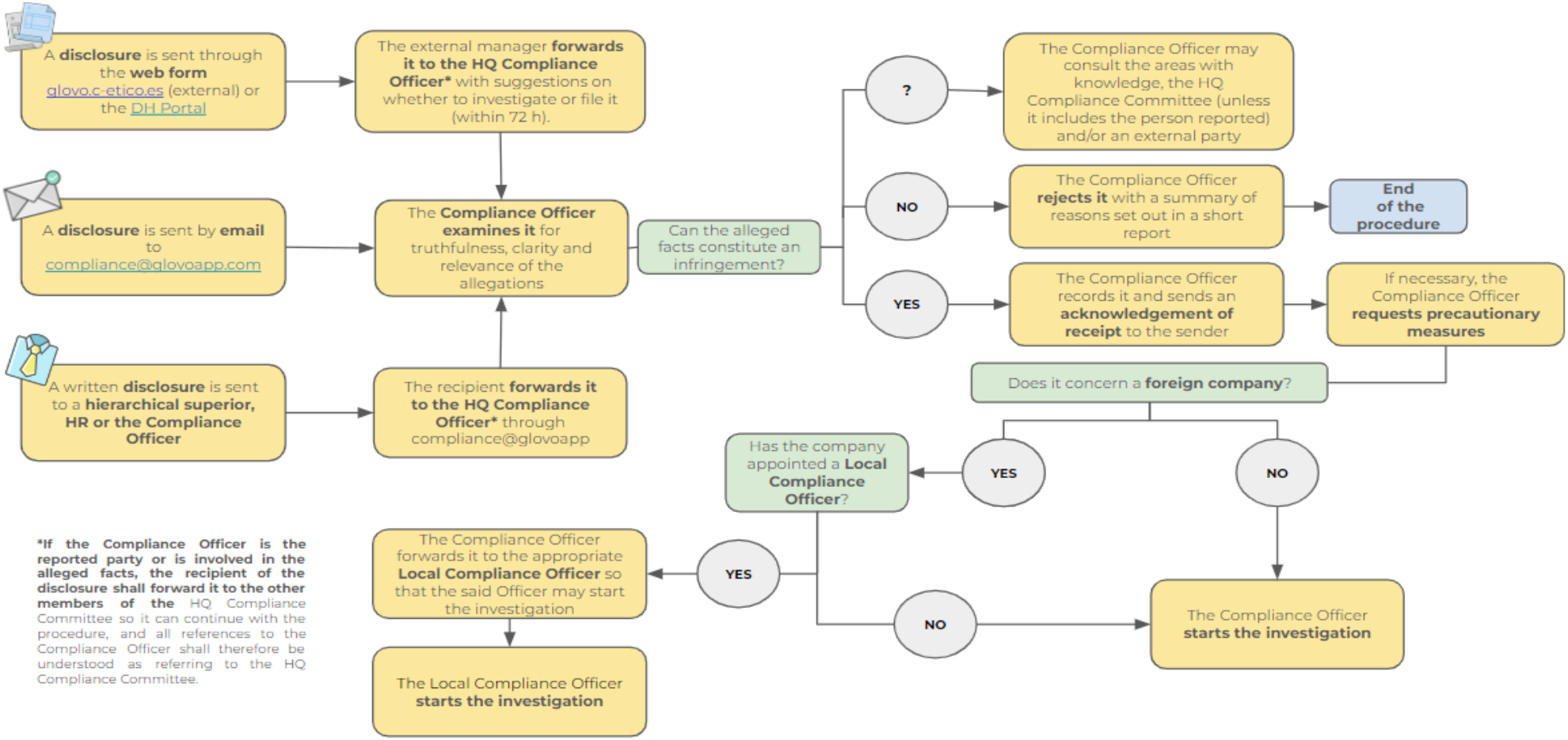
Policy Governance Framework	
Type	Policy
Revision period	Annually
Related documents	- Investigation Procedure - Disciplinary Procedure
Confidentiality	For Internal Use Only

Revision Log		
Version	Date of release	Description of changes
1.0	2020	Creation of the Whistleblower Policy
2.0	July 2021	Inclusion of further details in the content of the policy and changing the title (Ethics channel management Procedure)
3.0	June 2023	Modifications in order to align at Group Level with Delivery Hero and to adapt it to the European Directive on whistleblowers protection and local transpositions

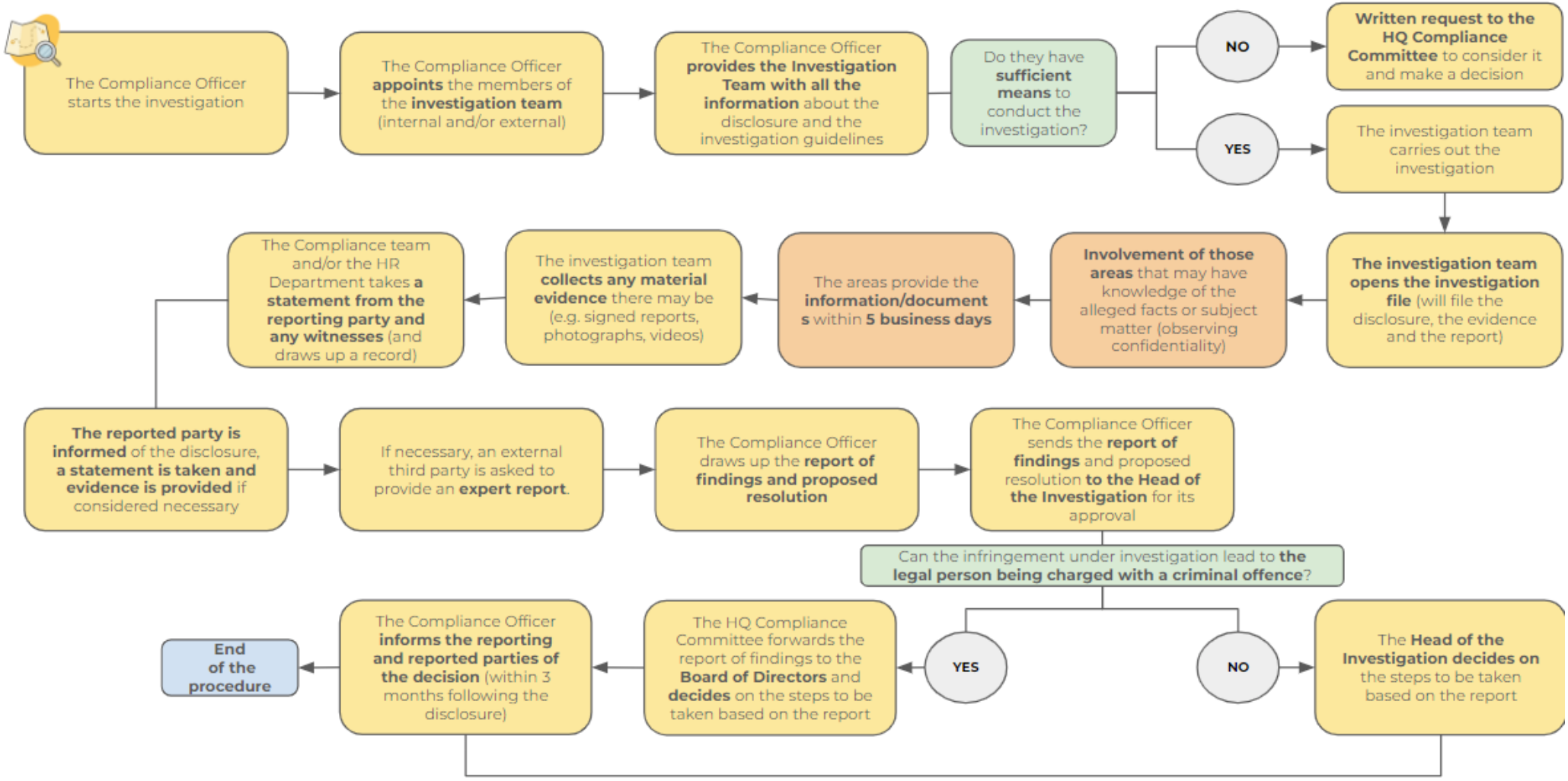
ANNEX I - Flow chart for queries



ANNEX II - Flow chart for disclosures



***If the Compliance Officer is the reported party or is involved in the alleged facts, the recipient of the disclosure shall forward it to the other members of the** HQ Compliance Committee so it can continue with the procedure, and all references to the Compliance Officer shall therefore be understood as referring to the HQ Compliance Committee.


The Compliance Officer starts the investigation
The Compliance Officer **appoints** the members of the **investigation team** (internal and/or external)
The Compliance Officer **provides the Investigation Team with all the information** about the disclosure and the investigation guidelines
Do they have **sufficient means** to conduct the investigation?
NO
Written request to the **HQ Compliance Committee** to consider it and make a decision
YES
The investigation team carries out the investigation
The investigation team opens the investigation file (will file the disclosure, the evidence and the report)
Involvement of those areas that may have knowledge of the alleged facts or subject matter (observing confidentiality)
The areas provide the **information/documents** within **5 business days**
The investigation team **collects any material evidence** there may be (e.g. signed reports, photographs, videos)
The Compliance team and/or the HR Department takes **a statement from the reporting party and any witnesses** (and draws up a record)
The reported party is informed of the disclosure, **a statement is taken and evidence is provided** if considered necessary
If necessary, an external third party is asked to provide an **expert report**.
The Compliance Officer draws up the **report of findings and proposed resolution**
The Compliance Officer sends the **report of findings** and proposed resolution **to the Head of the Investigation** for its approval
Can the infringement under investigation lead to **the legal person being charged with a criminal offence**?
YES
NO
The HQ Compliance Committee forwards the report of findings to the **Board of Directors** and **decides** on the steps to be taken based on the report
The **Head of the Investigation decides on** the steps to be taken based on the report
The Compliance Officer **informs the reporting and reported parties of the decision** (within 3 months following the disclosure)
End of the procedure

ANNEX III - Spain

1. Scope of Application

This Annex supplements the Ethics Channel Management Procedure, version 3.0, version date: June 2023, date of initial approval 15 of July 2021. This Annex applies to GLOVOAPP23, S.A. and its subsidiaries operating in Spain (hereinafter: "**Glovo Spain**" and/or "**Glovo**").

2. Designation of the person responsible for the management of the Ethics Channel

The Board of Directors will formally appoint the HQ Compliance Officer as the Responsible Person for managing the Ethics Channel and conducting the investigation. This appointment will be communicated to the Independent Authority for the Protection of Whistleblowers (in Spanish "Autoridad Independiente de Protección del Informante" or "A.A.I") by the channels that this authority designs to this effect. It will also be responsible for the registry of all the reports received to monitor them. He is also responsible for the record keeping of the reports and for their diligent follow-up.

3. Consultation to the employees' legal representation

In the companies that have employees' legal representation, a non-binding consultation will be carried out to the representatives so that they can contribute with considerations, if it deems so.

4. Communication of Disclosures in oral form

In addition to the procedure regulated in Section 7 of this Procedure, the Disclosure or Query submitted will be considered valid if it contains information on the Reporting person, information on the breach, information on the reported authority, or the person responsible for the breach.
The reporting person can also request a meeting in person with the Compliance Officer, in which case, the Compliance Team will arrange the meeting no later than 7 days after the request.

5. Right of Information

The reporting person shall receive an acknowledgement of receipt within a maximum of seven (7) days from receipt of the disclosure in the Ethics Channel. In addition, the reporting person shall also receive feedback, within three (3) months following date acknowledgment of the receipt of the disclosure by Glovo (or if no acknowledgement was sent to the

reporting person, three (3) months from the expiry of the seven-day period after the report was made), on whether the complaint has been admitted for processing and the outcome of its investigation and, if applicable, on the action that has been planned or adopted. Said timeframe could be extended to a total of six (6) months due to the complexity of the reported case.

6. Personal Data Protection

Personal data contained in the reports will be processes in accordance with the established in this Procedure. If the disclosure has not resulted in any action, the information may only be kept in the Ethics Channel in anonymized form, without the blocking obligation provided for in article 32 of Organic Law 3/2018, of December 5, being applicable.

7. External reporting channels

Whereas Glovo encourages the preferent use of the internal Ethics Channel available for disclosing potential breaches, Glovo employees have also available an external reporting channel to the Independent Authority for the Protection of Whistleblowers (in Spanish "Autoridad Independiente de Protección del Informante" or "A.A.I") or the authorities and regional bodies, in which the report will be received and managed outside Glovo, such as:

Cataluña	Oficina Antifrau de Catalunya https://www.antifrau.cat/
Andalucía	Oficina Andaluza contra el Fraude y la Corrupción https://antifraudeandalucia.es/
Comunidad Valenciana	Agencia Valenciana Antifrau https://www.antifraucv.es/buzon-de-denuncias-2/
Islas Baleares	Oficina de prevenció i lluita contra la corrupción a les Illes Balears https://www.oaib.es/
Navarra	Oficina de buenas prácticas y anticorrupción

8. Communication of potential criminal offences to the Public Prosecutor Office

If the facts disclosed can be constitutive of a criminal offence according to the Spanish Criminal Code, Glovo will immediately refer the report to the Spanish Public Prosecutor Office and the European Public Prosecutor Office if the facts can affect financial interests of the European Union, preserving the rights granted by Law.

9. Support measures

Taking into account the circumstances of the case, Glovo can facilitate the support measures for the reporting person that deems appropriate and in accordance with the law.

10. Trainings

Employees will be trained on the main elements of the information system, including the obligation to refer any report they receive to the person responsible for the system and to maintain confidentiality.

ANNEX IV - Croatia

1. Introduction

This Annex supplements the Ethics Channel Management Procedure, version 3.0, version date: June 2023, date of initial approval 15 of July 2021, which is an internal act governing the protection of the persons reporting breaches i.e. the Whistleblowers within GLOVOAPP23, S.A. and all the subsidiaries in its corporate group. This Annex applies to GLOVOAPP TECHNOLOGY d.o.o., GLOVO INFRASTRUCTURE d.o.o. or its subsidiaries or any subsidiaries of the GLOVOAPP23, S.A. practicing in the Republic of Croatia (hereinafter: "Glovo Croatia" and/or "Glovo").

This Annex determines the procedure of handling queries and disclosures (hereinafter jointly: the Applications) where the Application is made in the territory of the Republic of Croatia as well as where it is made by a Croatian citizen or if the Application is in any way connected to the business practices of GLOVOAPP TECHNOLOGY d.o.o., GLOVO INFRASTRUCTURE d.o.o., their subsidiaries or any subsidiaries of the GLOVOAPP23, S.A. practicing in the Republic of Croatia.

The procedure for handling Applications is governed primarily by the provisions of this Annex supplemented by the Ethics Channel Management Procedure. When there is a conflict between the provisions of this Annex and the provisions of the Ethics Channel Management Procedure the provisions of this Annex shall prevail.

This Annex is in accordance with the following legislation:

(i) Croatian Whistleblower Protection Act (Official Gazette No. 46/2022, hereinafter, "**WPA**")

(ii) 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 (hereinafter, "**Whistleblower Protection Directive**")

(iii) Croatian Criminal Act (Official Gazette No. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21)

(iv) Croatian Trade Act (Official Gazette No. 87/2008., 96/2008., 116/2008., 116/2008., 76/2009., 114/2011., 68/2013., 30/2014., 32/2019., 98/2019., 32/2020.)

(v) Croatian Labour Act (Official Gazette No. 93/2014., 127/2017., 98/2019.)

(vi) Croatian Data Confidentiality Act (Official Gazette No. 79/2007., 86/2012.)

(vii) General Data Protection Regulation.

This Annex will be displayed within the business premises of Glovo Croatia, its website, and will be forwarded to all the employees by email.

2. The procedure

1. The procedure for making queries or disclosures is available to all Glovo's employees and any third parties who wish to report actions or omissions that are unlawful and relate to the scope of the WPA (hereinafter: "Reporting person").

2. The Application can be made through the email address compliance@glovoapp.com. The

Reporting person can also arrange a meeting in person with the National Compliance Officer if he/she so prefers.

3. The Applications made by the Reporting person will be received by the National Compliance Officer who will carry out the appropriate procedure.

4. Upon receiving the Application, the National Compliance Officer will:

   (i) inform the Reporting person about the receipt of the Application within 7 days from the day of the receipt

   (ii) without delay take all the necessary measures within their capacity to protection the Reporting person

   (iii) investigate the existence of the alleged breach

   (iv) provide feedback to the Reporting person as a rule within 30 days, but in any event in a period not longer than 90 days from the date of acknowledgment of receipt

   (v) if the breach is not resolved within GLOVOAPP TECHNOLOGY d.o.o., the National Compliance Officer will forward the Application to the competent public bodies authorized to act according to the content of the Application

   (vi) without delay, inform the Reporting person, in writing, of the outcome of the examination of the Application

   (vii) notify the Ombudsman, in writing, of the received Applications and the outcome of the proceedings within 30 days of deciding on the Application

   (viii) protect the identity of the Reporting person and the data received in the Application from unauthorized disclosure.

   (ix) provide clear and easily accessible information on the procedure for submitting an Application to the Ombudsman or the public body responsible for dealing with the content of the application.

5. If the Application involves a foreign country the National Compliance Officer will forward the application to Glovo's HQ Compliance Officer who shall forward the application to the competent Local Compliance Officer.

3. Protection of the Reporting persons

1. For this Annex, the Application shall mean any oral or written submission that contains information on the alleged breach.

2. The Application will be considered valid if it contains information on the Reporting person, information on the breach, information on the reported authority, or the person responsible for the breach.

3. The Application may be filed in written and oral form. The written form includes any form of communication that provides a written trace. Applications made orally are considered valid where they are done by telephone or other voice messaging system as

well as by an in-person meeting at the request of the Reporting person.

4. Regarding the information submitted there are two types of Applications, queries, and disclosures. Upon receiving either type of Application the National Compliance Officer will conduct the same handling procedure described in Article 2 of this Annex and will conduct an investigation with the same degree of diligence. Both Queries and Disclosures can be written and oral.

5. The queries shall include the following content, although certain sections are optional:

   (i) Details or some contact details of the person sending the communication (required)
   (ii) The company to which the query relates (required)
   (iii) A description of the query (required)
   (iv) Evidence (optional)

1. The disclosures shall include the following content, although certain sections are optional:

1. The reporting person's details (optional)
2. The company to which the facts relate if known (required)
3. Description of the facts (required)
4. Evidence (optional).

4. Record Keeping of the Applications

1. Reporting persons shall qualify for protection under the following conditions:

   (i) When submitting the Application, the Reporting person had reasonable grounds to believe that the information on breaches reported is true at the time of reporting and that such information falls within the scope of the WPA.

   (ii) The Reporting person reported either following the procedure established by this Annex or externally in accordance with Article 23 and Article 24 WPA or made a public disclosure in accordance with Article 26 WPA.

   The Reporting persons who reported a breach or publicly disclosed information in accordance with the above-mentioned conditions shall not be deemed in any way responsible for such reporting or to have violated any restriction on the disclosure of information.

2. Persons who anonymously reported or publicly disclosed information on irregularities, and who meet the conditions referred to in paragraph 1 of this Article have the right to protection if their identity subsequently becomes known in the future and or if retaliation is determined regardless of whether they submitted the application anonymously.

3. The Reporting persons who reported breaches that fall within the scope of authorities, offices, or agencies of the European Union have the right to the protection prescribed by this Annex under the same conditions as persons who submit the application to the competent external notification authority.

4.

5. The Procedure for Appointing the National Compliance Officer

1. The National Compliance Officer shall keep a record of all the Applications received, following confidentiality requirements provided in Article 8 of this Annex.

2. The Applications shall be kept in a permanent form. Oral Applications, made *via* telephone or any device suitable for creating an audio recording, will be recorded and maintained in a permanent form in one of the following ways:

    (i) an audio recording of the conversation in a permanent and accessible form
    (ii) a complete and accurate transcript of the interviews made by the National Compliance Officer

3. The audio recording of the Application will not be made without the explicit consent of the Reporting person. The National Compliance Officer will inform the Reporting person of the possibility that the Application might be recorded before the submission of the Application.

4. When the Reporting person requests an in-person meeting with the National Compliance Officer for the purpose of submitting the Application, the National Compliance Officer shall keep complete and accurate records of the meeting in a permanent and accessible form.

5. Upon issuing explicit consent of the Reporting person National Compliance Officer has the right to record the meeting in one of the following ways:

    (i) an audio recording of the conversation in a durable and accessible form; or
    (ii) an accurate record of the meeting drawn up by the staff responsible for handling the application.

6. The National Compliance Officer shall offer the Reporting person the possibility to check and correct the transcript of the meeting as well as to confirm the accuracy by signature.

6. The Procedure for Appointing the National Compliance Officer

1. The National Compliance Officer will be appointed on the proposal of at least 20% of the employees employed by GLOVOAPP TECHNOLOGY d.o.o.

2. In the case of several proposals made by employees for the appointment of the National Compliance Officer the proposal that has the support of the greater number of employees will prevail.

3. Where two or more proposals have the equal support of employees, priority will be given to the proposal that was received first.

4. The National Compliance Officer has a deputy. The deputy is appointed together with the

National Compliance Officer in the equivalent procedure.

5. GLOVOAPP TECHNOLOGY may appoint a National Compliance Officer and his deputy without a proposal from the 20% of the employees employed by GLOVOAPP TECHNOLOGY if such a proposal is not given.

6. The appointed National Compliance Officer and his deputy shall be dismissed without delay based on a request submitted by at least 20% of the employees employed by GLOVOAPP TECHNOLOGY.

7. GLOVOAPP TECHNOLOGY shall initiate the procedure for the appointment of a different National Compliance Officer and his deputy no later than 30 days from the day of the dismissal. Until the decision on the appointment of a new National Compliance Officer is made, the tasks of the trustee shall be performed by the deputy, unless circumstances indicate that it is necessary to appoint a third person to temporarily perform the duties of the National Compliance Officer.

8. The National Compliance Officer and his deputy must give written consent for the appointment.

7. Cooperation with Ombudsman

1. National Compliance Officer shall notify the Croatian Ombudsman of all the
Applications of alleged breaches received. The notification will contain information on how the Application was handled and the outcome of the investigation.

2. The abovementioned notice to the Croatian Ombudsman shall be made within 30 days from the day of deciding on the Application.

8. Confidentiality

The identity of the Reporting person, i.e. the data which allow his identity to be revealed and any other data stated in the Application are available only to the persons in charge of receiving such reports and their further processing and they must remain protected unless the Reporting person agrees to the disclosure of that information.

The identity of the Applicant and all other information referred to in paragraph 1 of this Article may be disclosed only if this is a necessary and proportionate obligation imposed by European Union law or national law in the context of investigations by national authorities or in the context of court proceedings, *inter alia* to protect the right of defense of the Reporting person.

Identity of the Reporting person and data based on which his/her identity can be revealed and any other data stated in the Application data may not be used or disclosed for purposes that go beyond what is necessary for proper investigation of the Application.

Disclosures made under the exception provided for in paragraph 2 of this Article shall be subject to appropriate safeguards under applicable European Union rules and national legislation. The authority revealing the identity of the Reporting person shall inform him before disclosing his identity unless such information would jeopardize related investigations or court proceedings. When notifying the competent authorities, the

National Compliance Officer shall send a written notification stating the reasons for the disclosure of confidential information.

The provisions of this Article relating to the protection of the identity of the Reporting person shall also apply to the protection of the identity of the reported person.

The provision of paragraph 2) of the Introduction of the Glovo's Ethics Channel Management Procedure does not apply to the territory of the Republic of Croatia

The Annex as well as the Ethics Channel Management Procedure or any other act made by GLOVOAPP23, S.A., GLOVOAPP TECHNOLOGY d.o.o., GLOVO INFRASTRUCTURE d.o.o. or any of its subsidiaries does not prescribe any criminal sanction under Croatian law.

ANNEX V - Slovenia

1. Introduction

1. This Annex supplements the Ethics Channel Management Procedure, version 3.0, version date: June 2023, date of initial approval 15 of July 2021, which is an internal act governing the protection of the persons reporting breaches, i.e. the whistleblowers, within GLOVOAPP23, S.A. and all the subsidiaries in its corporate group. This Annex applies to Glovoapp SI, inovativne tehnološke rešitve, d.o.o. or any subsidiaries of the GLOVOAPP23, S.A. practicing in the Republic of Slovenia (hereinafter: "***Glovo Slovenia***").

2. This Annex determines only the procedure for handling Disclosures (hereinafter: "***Application***") which pertain to a breach of laws applicable in the Republic of Slovenia.

3. The procedure for (i) submitting, handling and answering Queries, and (ii) for submitting, handling and investigating Disclosures pertaining to a breach of laws other than those applicable in the Republic of Slovenia, in each case as set forth in the Ethics Channel Management Procedure, version 4.0, version date: July 2021, remains unaffected by this Annex.

4. The procedure for handling Applications is governed primarily by the provisions of this Annex supplemented by the Ethics Channel Management Procedure. Regardless of any provisions to the contrary under the Ethics Channel Management Procedure, if there is a conflict between the provisions of this Annex and the provisions of the Ethics Channel Management Procedure, the provisions of this Annex shall prevail.

5. This Annex is based on the following legislation:

   (i) Whistleblowers Protection Act (Official Gazette of RS, no. 16/2023; hereinafter: "***ZZPri***");

   (ii) 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 (hereinafter: "***Whistleblowers Protection Directive***");

   (iii) Criminal Code (Official Gazette of RS, no. 50/12 as amended; hereinafter: "***KZ-1***");

   (iv) Personal Data Protection Act (Official Gazette of RS, no. 163/22; hereinafter: "***ZVOP-2***");

   (v) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter: "***GDPR***");

   (vi) Public Information Access Act (Official Gazette of RS, no. 51/06 as amended; hereinafter: "***ZDIJZ***");

   (vii) Classified Information Act (Official Gazette of RS, no. 50/06 as amended; hereinafter: "***ZTP***");

6. This Annex will be displayed within the business premises of Glovo Slovenia, its website, and it will be forwarded to all its employees by email.

2. The Application and the procedure

1. For the purposes of this Annex, the Application shall mean any oral or written submission that contains information on the alleged breach of laws applicable in the Republic of Slovenia in the work environment within or related to Glovo Slovenia.

2. This procedure for making Applications is available to all employees of Glovo Slovenia and any other natural persons who wish to report information about a breach of laws applicable in the Republic of Slovenia which they detected within their work environment (hereinafter: "***Reporting person***").

3. "Work environment" shall mean a present or past employment or similar relationship in the context of which the Reporting person obtains information about the breach and in the context of which the Reporting person could suffer retaliation if he/she were to report the breach.

4. The Application can be made through the web form glovo.c-etico.es, the email address compliance@glovoapp.com, or the DH portal.

5. The Compliance Officer responsible for handling Applications in relation to Glovo Slovenia is the HQ Compliance Officer (hereinafter: "***National Compliance Officer***").

6. For the purposes of receiving the Applications and forwarding them to the National Compliance Officer, Glovo cooperates with an external Application Acceptance Service Provider (hereinafter: "***external service provider***"). The external service providers of Glovo is Ribas y Asociados, glovo.c-etico.es.

7. The Applications made by the Reporting person will be received by:

    - The external service provider, if submitted via the web form glovo.c-etico.es, such Applications will be forwarded to the National Compliance Officer; or
    - The National Compliance Officer, if submitted via the email address compliance@glovoapp.com, the DH portal or directly to the National Compliance Officer.

8. The Applications, which are received by the external service provider, are forwarded immediately to the National Compliance Officer. Regardless of anything to the contrary under the Ethics Channel Management Procedure, the National Compliance Officer is the only one to send the Acknowledgement of receipt to the Reporting person, carry out the appropriate investigations, compile a report and to inform the Reporting person on the findings of the procedure.

9. Upon receiving the Application, the National Compliance Officer will:

    i. Enter the Application in the Record of Disclosures, whereby the National Compliance Officer shall take into account the prohibition of identity disclosure and confidentiality when doing so.

    ii. Within 7 days of the receipt of the Application, assess if the application meets all the criteria for it to be examined, i.e. if:

        - It was made by a physical person;
        - The information relates to breach of any law applicable and valid in

the Republic of Slovenia, that was obtained by the Reporting person in his or her work environment;
- The reported information is not clearly untrue; and
- The Reporting person submitted this Application within 2 years of the alleged breach.

iii. Issue and serve to the Reporting person an Acknowledgement of receipt (containing, inter alia, the date and exact time of its receipt) within 7 days after receiving the Application, if the Application meets all the above criteria;

Or;

If the Application does not meet the above criteria or if the investigation into the breach would be pointless due to the minor or non-existing consequences of the breach, within 7 days after receiving the Application, inform the Reporting person of the reasons why the Application will not be examined. In such case, the National Compliance Officer is not required to take any further steps. However, although the Application does not meet the above criteria, the National Compliance Officer may take whatever action he/she considers necessary to address the breach, if he/she considers this necessary due to e.g. the severe nature of the alleged breach.

iv. Obtain all information that would be helpful in drafting proposals to remedy the breach or preventing harmful consequences of the breach, as well as to prevent any future breaches.

v. Investigate the existence of the alleged breach in a diligent, confidential and independent manner. The National Compliance Officer is not bound by any instructions in a particular case when investigating the breach.

vi. Cooperate with the Authority competent for conducting the external procedure whenever this is necessary for the processing of an Application before the National Compliance Officer or the Authority competent for conducting the external procedure.

vii. Provide to the Reporting person all information on protection of whistleblowers under the ZZPri and the remedies available to whistleblowers in the event of retaliation, information on the external procedure, etc.

viii. Take all necessary measures within his/her capacity to stop the alleged breach; or, if it is not within his/her competence to remedy the breach, inform in writing the persons responsible for remedying the breach (i) of its report and (ii) the proposed measures.

ix. Complete the processing of the Application within 3 months of the receipt.

x. Draw up a Report upon the end of the procedure. The Report should state if and why the Application was successful or not. If the Application was successful, the Report should state, inter

alia, what were the measures proposed and implemented to bring the breach to an end, to remedy the consequences of the breach and to prevent further breaches. The Report should also include the findings of the assessment of the effectiveness of the measures implemented and a list of any suggested or implemented measures for the protection of the Reporting person's identity.

xi. Immediately upon end of the procedure, inform the Reporting person, thereof and of the outcome of the procedure.

xii. Within three months of the start of the respective procedure inform the Reporting person of the end and outcome of the procedure; or in case the procedure is still pending, inform the Reporting person of the state of the proceedings.

xiii. Inform the Management of Glovo Slovenia of the findings of the report in writing, always taking into account the protection of the identity of the Reporting person.

3. Protection of the Reporting persons

1. If the Application is anonymous, the National Compliance Officer is not obliged to send any notifications to the Reporting person, unless he/she provided an address to which the information should be sent.

2. The Reporting person shall qualify for protection under the following conditions:

   (i) When submitting the Application, the Reporting person had reasonable grounds to believe that the information on the breaches reported is true at the time of reporting and if such information falls within the scope of the ZZPri.

   (ii) The Reporting person reported either following the procedure established by this Annex or externally in accordance with chapter 5 of the ZZPri or made a public disclosure in accordance with chapter 6 of the ZZPri.

   (iii) The Reporting person submitted this Application within 2 years of the alleged breach.

3. The Reporting person who reported anonymously and meets the conditions under paragraph 1 of this Clause, has the right to protection if his/her identity subsequently becomes known in the future.

4. Glovo Slovenia or Glovo HQ (and any of its employees) are not allowed to (try to) identify the Reporting person.

5. The Reporting person who reported either following the procedure established by this Annex or externally in accordance with chapter 5 of the ZZPri or made a public disclosure in accordance with chapter 6 of the ZZPri shall not be deemed in any way responsible for such reporting or to have any restrictions on the disclosure of information.

6. As a consequence of making the Application, the Reporting person may

not be subject to any retaliatory measures, inter alia:

- Dismissal or suspension
- Demotion or refusal to promote;
- Relocation of the job location, transfer/change of job scope/description, change of working times, reduction of working hours/scope, non-payment or delay of payment of salary or other benefits, bonuses or severance pay;
- Refusal to provide training;
- Negative assessments at work, or giving bad references;
- Disciplinary action;
- Harassment or intimidation;
- Discrimination or unfavourable treatment;
- Non-renewal of a temporary contract, or non-conversion into a permanent contract;
- Termination of a temporary contract prior to the expiry of the term of such contract;
- Arbitrary actions of the employer, including actions which inflict damages on the Reporting person (including reputation and monetary damage or loss of income/profit);A
- Terminating a contract for the procurement of goods or services prematurely (i.e. prior to the end of term of cush contract);
- Revocation of licence or permit;
- Arbitrary imposing of medical examinations;
- Replacing the terms of employment or retirement with less favourable terms;
- Reputational damage or blacklisting;
- Posting the employee to a different place without justification, or refusing a transfer;
- Refusing to give the employee an appointment in relation to a service or position;
- Filing malicious legal actions against the Reporting person.

An attempt or threat of retaliatory measure shall also constitute a prohibited retaliatory measure.

4. Record keeping of the Applications

1. The National Compliance Officer shall keep a Record of all Applications received (hereinafter: "***Record***"). The National Compliance Officer should duly enter each Application in the said Record whilst complying with prohibition on disclosure of identity and confidentiality.

2. Oral Applications should be either:

   - Accurately summarised in a written transcript; or
   - Recorded, provided that the Reporting person gave his/her explicit consent.

3. The National Compliance Officer shall offer the Reporting person the possibility to check and correct the transcript of the oral Application as well as to confirm its accuracy by signature.

4. The Record should include the following information: information (such as, e.g. name – if provided, pseudonym, address, telephone number etc.) of the Reporting person, the persons concerned, and any person that could help with resolving the Application, any documentation that was submitted by any of the mentioned persons and any documentation acquired in the procedure (including the transcript or record of the oral Application).

5. The National Compliance Officer shall keep the personal data in the Record for 5 years after the procedure following the Application has been resolved. After 5 years, the data should be destroyed.

6. Personal data that is clearly not necessary to process the Application should not be processed. If any such unnecessary data is obtained by mistake, it should be immediately deleted.

7. The Record, especially the personal data therein, must not be accessible to any unauthorised person.

5. Confidentiality

1. Without the Reporting person's explicit consent, no one is allowed to disclose the identity of the Reporting person to anyone, other than the National Compliance Officer and the competent public authorities for external reporting. This applies to all information from which the identity of the Reporting person could be revealed. The Reporting person should be informed in advance of any such identity reveals.

2. Notwithstanding the provision of the preceding paragraph, the Reporting person's identity may be disclosed to the State Prosecutor upon the latter's request, if this is indispensable to investigate a criminal act, or to the Court at the latter's request, if this is necessary for court proceedings. If the Reporting person's identity is disclosed in accordance with the preceding sentence, the Reporting person must be informed thereof in advance in writing and with stating the reasons for such disclosure, unless the State Prosecutor or the Court finds that such notice would jeopardise an investigation or court procedure.

3. Notwithstanding the provisions of paragraph one and two of this Clause 5 above, the identity of the Reporting person may not be disclosed if this would endanger life or seriously jeopardise the public interest or national defence.

4. The National Compliance Officer and all other persons shall at all times protect the confidentiality of the identity of the Reporting person.

6. Submission of an external report in accordance with chapter 5 of the ZZPri

1. The Reporting person may report the breach directly to an external authority, if:

(i) There is no internal procedure/channel in place;
(ii) The Application could not be dealt with effectively in the internal procedure;
(iii) The Reporting person is of the opinion that he/she may face the risk of retaliation if making the Application using the internal channel.

2. An external report can be lodged in accordance with chapter 5 of the ZZPri with the following authorities:

- The Agency for Communication Networks and Services of the Republic of Slovenia;
- The Securities Market Agency;
- The Slovenian Competition Protection Agency;
- The Slovenian Traffic Safety Agency;
- Insurance Supervision Agency;
- Public Audit Oversight Agency;
- The Bank of Slovenia;
- National Review Commission for Reviewing Public Procurement Procedures;
- Financial Administration;
- Market Inspectorate;
- Office for Money Laundering Prevention;
- The Information Commissioner;
- Information Security Inspection Service;
- Radiation and Nuclear Safety Inspection Service;
- Radiation Protection Inspection Service;
- Inspection for Food Safety, Veterinary Sector and Plant Protection;
- Labour Inspectorate;
- Public Sector Inspectorate;
- Natural Resources and Spatial Planning Inspectorate;
- Agency for Medicinal Products and Medical Devices of the Republic of Slovenia;
- Supervisory authorities in accordance with the rules governing the use of European cohesion policy funds in the Republic of Slovenia;
- Health Inspectorate;
- The company Slovenski državni holding d.d.; or
- Commission for the Prevention of Corruption.

3. The provision of paragraph 3 of chapter 1 of the Introduction of the Ethics Channel Management Procedure does not apply to Applications related to breaches of laws applicable in Slovenia.

4. The provisions of this Annex and the Ethics Channel Management Procedure shall be without prejudice to any rights and obligations of Glovo Slovenia or Reporting persons under the law governing criminal procedure or the law governing the protection of classified information.

ANNEX VI - Bulgaria

1. Introduction

1. This Annex VI supplements the Ethics Channel Management Procedure, version 3.0, version date: June 2023, date of initial approval 15/07/2021, which is an internal act governing the protection of the persons reporting breaches i.e. the whistleblowers within GLOVOAPP23, S.A. and all the subsidiaries in its corporate group. This Annex VI applies to GLOVOAPP BULGARIA EOOD, its subsidiaries (if any) and the subsidiaries of the GLOVOAPP23, S.A. with business activities on the territory of Bulgaria (hereinafter: "Glovo Bulgaria" and/or "Glovo").

2. This Annex VI determines the procedure of handling queries and disclosures (hereinafter jointly: the Applications) where the Application is made on the territory of Bulgaria, is made by a Bulgarian citizen or if the Application is with respect to the business activities of Glovo, its subsidiaries (if any) or the subsidiaries of GLOVOAPP23, S.A. with business activities in Bulgaria.

3. The procedure for handling Applications is governed primarily by the provisions of this Annex VI, supplemented by the Ethics Channel Management Procedure. When there is a conflict between the provisions of this Annex VI and the provisions of the Ethics Channel Management Procedure, the provisions of this Annex VI shall prevail.

4. This Annex VI is in accordance with the following legislation:

(i) The Bulgarian **"Law on protection of persons reporting or publicly disclosing information on breaches"**. (Official Gazette No. 11/2023, hereinafter, the "LAW")

(ii) **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 (hereinafter, the "Directive")

5. This Annex VI will be displayed within the business premises of Glovo, its website and it will be forwarded to all the employees by email. It will also be brought to the attention of the suppliers and contractors of Glovo.

6. The Directive and the Law provide protection to whistleblowers with regards to:

(i) Breaches in the following areas:

➢ public procurement;

➢ financial services, products and markets and prevention of money laundering and terrorist financing;

➢ products safety and compliance;

➢ transport safety;

➢ protection of the environment;

➢ radiation protection and nuclear safety;

➢ food and feed safety, animal health and welfare;

➢ public health;

➢ consumer protection;

➢ protection of privacy and personal data; and

➢ security of network and information systems;

(ii) Breaches affecting the financial interests of the EU as referred to in Art. 325 of the Treaty on the (ii) Breaches affecting

the financial interests of the EU as referred to in Art. 325 of the Treaty on the

Functioning of the European Union ("TFEU") and as further specified in relevant EU measures.

(iii) Breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of EU and

Bulgarian competition and state aid rules.

(iv) Breaches relating to cross border tax schemes or arrangements, the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

(v) Information on the commission of a general offense, which the whistleblower has obtained in the process of performing its work-related obligations.

(vi) Breaches of the Bulgarian legislation in the following areas:

➢ payment regulations for public and municipal fees;

➢ labor legislation, and

➢ legislation related to the performance of public service.

2. The procedure

1. The procedure for making queries or disclosures is available to all Glovo employees and any third parties who wish to report actions or omissions that are unlawful and relate to the scope of the LAW (hereinafter: "Reporting person").

2. The Application can be made through the [...][AT1] email address or by telephone on the telephone number: [...]. The Reporting person can also arrange for a meeting in person with the person or persons, responsible for the receipt and processing of Applications (hereinafter: "Responsible person") if he/she so prefers.

3. The Applications made by the Reporting person will be received by the Responsible person who will carry out the appropriate investigation procedure.

4. Upon receiving the Application, the Responsible person will:

(i) inform the Reporting person about the receipt of the Application within 7 days from the day of the receipt;

(ii) without delay take all the necessary measures within their capacity to protect the Reporting person;

(iii) investigate the existence of the alleged breach;

(iv) provide feedback to the Reporting person as a rule within 30 days, but in any event in a period not longer than 90 days from the date of acknowledgment of receipt;

(v) Contact and cooperate with all relevant bodies within Glovo in order to resolve the breach;

(vi) Consult the Reporting person on contacting the relevant public bodies when his/her rights have been violated;

(vii) without delay, inform the Reporting person, in writing, of the outcome of the examination of the Application;

(viii) protect the identity of the Reporting person and the received data from unauthorized disclosure;

(ix) provide clear and easily accessible information on the procedure for

submitting an Application to the External channel or the public body responsible for dealing with the content of the application.

5. If the Application involves a foreign country, the Responsible person will forward it to Glovo's HQ Compliance Officer who shall forward the application to the competent local Responsible person.

3. Validity of the Application

1. With respect to this Annex VI, an 'Application' shall mean any oral or written submission that contains information on the alleged breach.

2. The Application will be considered valid if it contains information on the Reporting person, information on the breach, information on the reported authority, or the person responsible for the breach.

3. The Application may be filed in written and oral form. The written form includes any form of communication that provides a written trace. Applications made orally are considered valid where they are done by telephone or other voice messaging system as well as by an in-person meeting at the request of the Reporting person.

4. Regarding the information submitted there are two types of Applications, queries, and disclosures. Upon receiving either type of Application the Responsible person will conduct the same handling procedure described in Article 2 of this Annex and will conduct an investigation with the same degree of diligence. Both Queries and Disclosures can be written and oral.

5. The queries shall include the following content:

(i) Details or some contact details of the person sending the communication (required);

(ii) The company to which the query relates, if known (required);

(iii) A description of the query (required);

(iv) Evidence (optional).

6. The disclosures shall include the following content, although certain sections are optional:

(i) The reporting person's details (required)

(ii) The company to which the facts relate if known (required)

(iii) Description of the facts (required)

(iv) Evidence (required).

4. Protection of the Reporting Persons

1. Reporting persons shall qualify for protection under the following conditions:

(i) When submitting the Application, the Reporting person had reasonable grounds to believe that the information was true at the time of reporting and that such information falls within the scope of the LAW; and

(ii)The Reporting person reported either following the procedure established by this Annex VI externally in accordance with Section 2 of the LAW or made a public disclosure.

The Reporting persons who reported a breach or publicly disclosed information in accordance with the above-mentioned conditions shall not be deemed in any way

responsible for such reporting or to have violated any restriction on the disclosure of information as long as the act of obtaining the information was not in itself a crime.

2. Persons who anonymously publicly disclosed information on irregularities, and who meet the conditions referred to in paragraph 1 of this Article have the right to protection if their identity subsequently becomes known in the future and or if retaliation is determined regardless of whether the public disclosure was anonymous.

3. The protection, provided by the Directive and the LAW, extends to any persons (natural or legal) which are related to the Reporting person.

5. Record Keeping of the Applications

1. The Responsible person shall keep a record of all the Applications received, following the confidentiality requirements, provided in Article 8 of this Annex VI.

2. The Applications shall be kept in a permanent form. Oral Applications, made via telephone or via any device suitable for creating an audio recording, will be recorded and maintained in a permanent form in one of the following ways:

(i) an audio recording of the conversation in a permanent and accessible form

(ii) a complete and accurate transcript of the interviews made by the Responsible person.

3. The audio recording of the Application will not be made without the explicit consent of the Reporting person. The Responsible person will inform the Reporting person of the possibility that the Application might be recorded before the submission of the Application.

4. When the Reporting person requests an in-person meeting with the Responsible person for the purpose of submitting an Application, the latter shall keep complete and accurate records of the meeting in a permanent and accessible form.

5. Upon issuing explicit consent of the Reporting person the Responsible person has the right to record the meeting in one of the following ways:

(i) an audio recording of the conversation in a durable and accessible form; or

ii) an accurate record of the meeting drawn up by the Responsible persons.

6. The Responsible person shall offer the Reporting person the option to check and correct the transcript of the meeting as well as to confirm the accuracy by signature.

6. The Procedure for Appointing the Responsible person

1. The Responsible person shall be appointed by the company and shall administer the Internal Channel of Glovo for Bulgaria in accordance with the LAW.

2. The Responsible person shall register him or herself with the Commission for Personal Data Protection, as described on the website of the latter.

3. The Responsible person may hold a different position in the company in

addition to his/her duties as per this Annex VI.

7. Cooperation with the Commission for Personal Data Protection

1. The Responsible person shall notify the Commission of all the Applications on alleged breaches received on a regular basis. The notification will contain information on the number of Applications, on how they were handled and the outcome of the investigation.

8. Confidentiality

1. The identity of the Reporting person, i.e. the data which allows his/her identity to be revealed and any other data stated in the Application are available only to the Responsible person in charge of receiving the Applications and their further processing, and they must remain protected unless the Reporting person agrees to the disclosure of that information.

2. The identity of the Reporting person and all other information referred to in paragraph 1 of this Article may be disclosed only if this is a necessary and proportionate obligation imposed by European Union or Bulgarian law in the context of investigations by national authorities or in the context of court proceedings, inter alia to protect the right of defense of the Reporting person.

3. The Identity of the Reporting person and data based on which his/her identity can be revealed and any other data stated in the Application data may not be used or disclosed for purposes that go beyond what is necessary for the investigation.

4. Disclosures made under the exception provided for in paragraph 2 of this Article shall be subject to appropriate safeguards under applicable European Union rules and the Bulgarian legislation. The authority revealing the identity of the Reporting person shall inform him/her before disclosing his/her identity unless such information would jeopardize related investigations or court proceedings. When notifying the competent authorities, the Responsible person shall send a written notification stating the reasons for the disclosure of confidential information.

5. The provisions of this Article relating to the protection of the identity of the Reporting person shall also apply to the protection of the identity of the reported person.

The provision of paragraph 2) of the Introduction of the Glovo's Ethics Channel Management Procedure does not apply to the territory of Bulgaria.

ANNEX VII - Romania

1. Introduction

1. This Annex supplements the Ethics Channel Management Procedure, version 3.0, version date: June 2023, date of initial approval 15 of July 2021, which is an internal act governing the protection of the persons reporting breaches - i.e., the Whistleblowers within GLOVOAPP23, S.A. and all the subsidiaries in its corporate group.

This Annex applies to GLOVOAPPRO S.R.L. , GLOVO INFRASTRUCTURE SERVICES RO S.R.L. or its subsidiaries or any subsidiaries of the GLOVOAPP23, S.A. operating in Romania (jointly mentioned hereinafter as "Glovo Romania" and/or "Glovo").

2. This Annex determines the procedure of handling queries and disclosures (hereinafter jointly: the Applications) where the Application is made in the territory of Romania as well as where it is made by a Romanian citizen or if the Application is in any way connected to the business practices of GLOVOAPPRO S.R.L., GLOVO INFRASTRUCTURE SERVICES RO S.R.L., their subsidiaries or any subsidiaries of the GLOVOAPP23, S.A. practicing in Romania.

3. The procedure for handling Applications is governed primarily by the provisions of this Annex supplemented by the Ethics Channel Management Procedure. When there is a conflict between the provisions of this Annex and the provisions of the Ethics Channel Management Procedure the provisions of this Annex shall prevail.

4. This Annex is in accordance with the following legislation:

(i) Law no. 361/2022 on the protection of whistleblowers in the public interest (hereinafter, "**Law 361/2022**")

(ii) 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 (hereinafter, "**Whistleblower Protection Directive**")

(iii) Romanian Labour Code

(iv) Romanian Criminal Code

(v) General Data Protection Regulation

(vi) as well as any special rules regarding the reporting of non-observance of the laws included in the Romanian pieces of legislation in the fields of consumer protection, product safety and compliance, financial services, products and markets, and prevention of money laundering and terrorist financing, transport safety, etc.

5. The scope of this Annex does not include the disclosure of facts, information or documents, regardless of their form, which is prohibited by the provisions relating to public procurement in the fields of defense and national security.

6. This Annex will be displayed within the business premises of Glovo Romania, its website, and will be forwarded to all the employees by email.

2. The procedure

1. The procedure for making queries or disclosures is available to all Glovo's employees and any third parties who wish to report actions or omissions that are unlawful and relate to the scope of the Law 361/2022 (hereinafter: "Reporting person").
2. The Application can be made through the following ways:
   (1) through a dedicated email address compliance@glovoapp.com.;

(2) Through the DH Portal which can be accessed from the following link.
(3) by submitting The Risk or Noncompliance Communication Form which can be accessed from the following link: https://glovo.c-etico.es/?locale=ro;
(4) in printed form, by postal mail, addressed to the Romanian Compliance Officer at the Glovo's headquarters address: Bucharest, Calea Șerban Vodă, nr. 206, Etaj 4, Clădirea U-Center, District 4,
(5) The Reporting person can also arrange a meeting in person with the Romanian Compliance Officer if he/she so prefers.

3. The Applications made by the Reporting person will be received by the Romanian Compliance Officer who will carry out the appropriate procedure.
4. Upon receiving the Application, the Romanian Compliance Officer will:

(i) inform the Reporting person about the receipt of the Application within 7 (seven) calendar days from the day of the receipt,
(ii) without delay take all the necessary measures within their capacity to protection the Reporting person,
(iii) investigate the existence of the alleged breach,
(iv) provide feedback to the Reporting person as a rule within 30 calendar days, but in any event in a period not longer than 90 calendar days from the date of acknowledgment of receipt, or, if no acknowledgement was sent to the Reporting person, three months from the expiry of the seven-day period after the Application was made, as well as, subsequently, whenever developments are recorded in the conduct of subsequent actions, except in the case where the information could jeopardize their conduct,
(v) if the breach is not resolved within Glovo Romania, the Romanian Compliance Officer will forward the Application to the competent public bodies authorized to act according to the content of the Application,
(vi) without delay, inform the Reporting person, in writing, of the outcome of the examination of the Application,
(vii) protect the identity of the Reporting person and the data received in the Application from unauthorized disclosure,
(viii) provide clear and easily accessible information on the procedure for submitting an Application through the external channels to the National Integrity Agency or the public body responsible for dealing with the content of the Application.

5. In the event of submitting an anonymous Application which does not contain sufficient information regarding violations of the legislation in order to allow the analysis and resolution of the Application, and the Romanian Compliance Officer has requested its completion within 15 days, without this obligation being fulfilled, the Romanian Compliance Officer has the right to cease the solving procedure.

6. The Romanian Compliance Officer may decide to close the procedure if, after reviewing the Application, it is determined that it is clearly a minor breach and does not require further follow-up action other than closing the procedure. This provision is without prejudice to the obligation to maintain confidentiality, to inform the Reporting person, and is without prejudice to other obligations or other applicable procedures to remedy the reported alleged breach.

7. If the Application involves a foreign country the Romanian Compliance Officer will forward the application to Glovo's HQ Compliance Officer who shall forward the Application to the competent Local Compliance Officer.

3. Validity of the Application

1. For this Annex, the Application shall mean any oral or written submission that contains information on the alleged breach.

2. The Application will be considered valid if it contains, at least, the following:

(i) information on the Reporting person: name and surname, contact details of the Reporting person, the professional context in which the information was obtained, the date and signature, as the case may be;

(ii) information on the breach: the description of the act likely to constitute a breach, as well as, as the case may be, the evidence in support of the Application;

(iii) information on the person responsible for the breach, if known.

3. An Application that does not include the name, surname, contact details or signature of the Reporting person is examined and resolved to the extent that it contains indications of the alleged breach.

4. The Application may be filed in written and oral form. The written form includes any form of communication that provides a written trace. Applications made orally are considered valid where they are done in an in-person meeting at the request of the Reporting person, in compliance with the requirements provided below at Article 5.

5. Regarding the information submitted there are two types of Applications, queries, and disclosures. Upon receiving either type of Application the Romanian Compliance Officer will conduct the same handling procedure described in Article 2 of this Annex and will conduct an investigation with the same degree of diligence. Both Queries and Disclosures can be written and oral and shall contain the elements provided above at point 2.

4. Protection of the Reporting Persons

1. Reporting persons shall qualify for protection under the following conditions:

When submitting the Application, the Reporting person had reasonable grounds to believe that the information on breaches reported is true at the time of reporting and that such infor
mation falls within the scope of the Law 361/2022.

The Reporting person reported either following the procedure established by this Annex or externally in accordance with Article 17 and Article 18 of the Law 361/2022or made a public disclosure in accordance with Article 19 of Law 361/2022.

The Reporting persons who reported a breach or publicly disclosed information in accordance with the above-mentioned conditions shall not be deemed in any way responsible for such reporting or to have violated any restriction on the disclosure of information. In particular, no retaliation, discrimination or penalty, direct or indirect, will affect those who have submitted an Application in good faith.

2. Persons who anonymously reported or publicly disclosed information on irregularities, and who meet the conditions referred to in paragraph 1 of this Article have the right to protection if their identity subsequently becomes known in the

future and or if retaliation is determined regardless of whether they submitted the Application anonymously.

3. The Reporting persons who reported breaches that fall within the scope of authorities, offices, or agencies of the European Union have the right to the protection prescribed by this Annex under the same conditions as persons who submit the application to the competent external notification authority.

5. Record Keeping of the Applications

1. The Romanian Compliance Officer shall keep a record of all the Applications received, following confidentiality requirements provided in Article 6 of this Annex.

2. The Applications shall be kept in a permanent form for 5 years. After the expiration of the 5-year storage period, they are destroyed, regardless of the support on which they are stored. Oral Applications made via in-person meeting will be recorded and maintained in a permanent form in one of the following ways:

(i) an audio recording of the conversation in a permanent and accessible form, subject to the consent of the Reporting person;
(ii) a complete and accurate transcript of the interviews made by the Romanian Compliance Officer

3. The audio recording of the Application will not be made without the explicit consent of the Reporting person. The Romanian Compliance Officer will inform the Reporting person of the possibility that the Application might be recorded before the submission of the Application.

4. When the Reporting person requests an in-person meeting with the Romanian Compliance Officer for the purpose of submitting the Application, the Romanian Compliance Officer shall keep complete and accurate records of the meeting in a permanent and accessible form accordingly with the legal requirements provided in point 2 above.

5. Upon issuing explicit consent of the Reporting person, the Romanian Compliance Officer has the right to record the meeting in one of the following ways:

(i) an audio recording of the conversation in a durable and accessible form; or
(ii) an accurate record of the meeting drawn up by the staff responsible for handling the Application, in a durable and accessible form, subject to the consent of the Reporting person.

6. The Romanian Compliance Officer shall offer the Reporting person the possibility to check and correct the transcript of the meeting as well as to confirm the accuracy by signature.

7. If the Reporting person does not consent to the transcription or recording of the conversation/meeting, he or she is directed to report in writing, on paper, to the Romanian Compliance Officer, or in electronic format, to the dedicated e-mail address.

6. Confidentiality

1. The identity of the Reporting person, *i.e.,* the data which allow his/her identity to be revealed directly or indirectly and any other data stated in the Application are available only to the persons in charge of receiving such Applications – i.e., the Romanian Compliance Officer, and their further processing and they must remain protected unless the Reporting person agrees to the disclosure of that information.

2. The identity of the Applicant and all other information referred to in paragraph 1 of this Article may be disclosed only if this is a necessary and proportionate obligation imposed by European Union law or Romanian law, in compliance with the conditions and limits provided by it, in the context of investigations by Romanian authorities or in the context of court proceedings, *inter alia,* to protect the right of defense of the Reporting person. The Reporting person is previously informed, in writing, about the disclosure of the identity and the reasons for the disclosure of the confidential data in question.

3. Identity of the Reporting person and data based on which his/her identity can be revealed and any other data stated in the Application data may not be used or disclosed for purposes that go beyond what is necessary for proper investigation of the Application.

4. Disclosures made under the exception provided for in paragraph 2 of this Article shall be subject to appropriate safeguards under applicable European Union rules and Romanian legislation. The authority revealing the identity of the Reporting person shall inform him/her before disclosing his identity unless such information would jeopardize related investigations or court proceedings.

5. The provisions of this Article relating to the protection of the identity of the Reporting person shall also apply to the protection of the identity of the reported person.

6. The obligation to ensure confidentiality is maintained even if the Application mistakenly reaches another person within Glovo Romania other than the Romanian Compliance Officer. In this case, the report is submitted immediately to the Romanian Compliance Officer.

7. Data Protection

Any personal and sensitive information contained in the Application, including those relating to the identity of the Reporting person or other individuals, must be processed in accordance with the applicable rules for the protection of personal data, as established by European and Romanian applicable legislation.

Data controller	GLOVOAPPRO S.R.L., GLOVO INFRASTRUCTURE SERVICES RO S.R.L. or its subsidiaries or any subsidiaries of the GLOVOAPP23, S.A. operating in Romania
Nature of the processing	Collection, recording, organization, structuring, storage, modification, extraction, consultation, use, communication by transmission, dissemination or any other form of provision, reconciliation or interconnection, limitation, destruction.
Legal basis of the processing	As the case may be; - legal obligation, - legitimate interest, - consent.
Purpose of the processing	The purpose of the processing is reception and resolving the wrongdoing presented by the Reporting person within the Application, as well as maintain statistics on reports regarding the non-compliance with the legal requirements, according to the Law 361/2022.

Type of personal data	The personal data may be: - identity, position and contact details of the Reporting person; - identity, positions, contact details of the persons who are the subject of the Application; - identity, positions and contact details of any third party mentioned in the Application; - identity, positions and contact details of persons involved in the collection or processing of the Application; - reported facts; - elements collected in the context of the verification of the reported facts, etc.
Category of data subjects	The data subjects are: - Reporting person; - presumed victims of the wrongdoing, if the case; - person targeted by an Application; - any third party mentioned in the Application; - persons involved in the collection or processing of the Application; - where applicable, persons questioned in the context of verification the information provided in the Application.

Rights of data subjects	Data Controller ensures the following rights of the data subjects in compliance with the GDPR Regulation: - Right of access to personal data; - Right to rectification of personal data; - Right to erasure of personal data ('right to be forgotten'); - Right to restriction of processing of personal data; - Right to object to the processing of personal data; - Right to data portability; - Right not to be subject to decisions based solely on automated processing, including profiling; - Right to lodge a complaint with the National Supervisory Authority for Personal Data Processing to the following link: www.dataprotection.ro.
Storage period	The supporting documentation pertaining the Application is archived, safely and for a period of 5 (five) years after the closing of the Application, after which they will be destroyed, regardless of the support on which they are being kept.

Requests to exercise the rights of data subjects shall be made to the following email address:

gdpr@glovoapp.com

8. Update of the Annex

This Annex will be regularly reviewed to ensure the alignment with the ever-changing regulatory or organizational requirements occurred over time.

9. Miscellaneous

The penalty applicable against the Reporting person, in case of Applications made with willful intent or gross negligence that are false, baseless, with defamatory content or otherwise made for the sole purpose of harming Glovo Romania or the ones affected by the Application is fined by the legislation in force with an amount of Lei 2,500 to Lei 30,000, if the deed was not committed under such conditions as to be considered, according to the law, a crime. Moreover, Glovo may claim damages.

The Annex as well as the Ethics Channel Management Procedure or any other act made by GLOVOAPP23, S.A., GLOVOAPPRO S.R.L.., GLOVO INFRASTRUCTURE SERVICES RO S.R.L. or any of its subsidiaries does not prescribe any criminal sanction under Romanian law.

ANNEX VIII - Portugal

1. Introduction

1.1. This Annex supplements the Ethics Channel Management Procedure, version 2.0, version date: July 2021, date of approval 15/07/2021, which is an internal act governing the protection of the persons reporting breaches, i.e. the Whistleblowers, within GLOVOAPP23, S.A. and all the subsidiaries in its corporate group. This Annex applies to GLOVOAPP PORTUGAL, UNIPESSOAL LDA. or any subsidiaries of GLOVOAPP23, S.A. practicing in Portugal (hereinafter: "Glovo Portugal" and/or "Glovo").

1.2. This Annex determines the local specificities where the Disclosure is made in Portugal as well as where it is in any way connected to the business practices of GLOVOAPP PORTUGAL, UNIPESSOAL LDA. or any subsidiaries of GLOVOAPP23, S.A. practicing in Portugal).

1.3. Reporting Person(s): Glovo makes available the Ethics Line to all its employees, job applicants, volunteers and trainees, manufacturers, suppliers or third parties with whom it has a direct relationship and a lawful business or professional interest, as well as any person working under their supervision and direction, and its shareholders and persons belonging to the administrative, management or supervisory body, including non-executive members. This Annex shall also apply to reporting persons where they report or publicly disclose information on breaches acquired in a work-based relationship which has since ended and to reporting persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

1.4. This Annex is in accordance with the following legislation:

(i) Law No. 93/2021, 20 December (Portuguese Whistleblower Protection Act).

(ii) Directive (EU) 2019/1937 of the European Parliament and the Council of 23 October 2019 on the protection of persons who report breaches of Union law (Whistleblower Protection Directive).

(iii) Law No. 58/2019 8 August (Portuguese Data Protection Law).

(iv) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

2. Local specificities

2.1. The Disclosure may relate to infringements that have been committed, are being committed or whose commission can reasonably be foreseen, as well as attempts to conceal such infringements.

2.2. In addition to what is stated in the Ethics Channel Management Procedure[1], the Reporting Persons may disclose:

(i) breaches falling within the scope of the Union acts set out in the Whistleblower

Protection Directive Annex that concern the following areas:

- public procurement;
- financial services, products and markets, and prevention of money laundering and terrorist financing;
- product safety and compliance;
- transport safety;
- protection of the environment;
- radiation protection and nuclear safety;
- food and feed safety, animal health and welfare;
- public health;
- consumer protection;
- protection of privacy and personal data, and security of network and information systems;

(ii) breaches affecting the financial interests of the Union as referred to in Article 325 TFEU and as further specified in relevant Union measures.

(iii) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

(iv) Violent crime, especially violent and highly organized crime, as well as the crimes provided for in paragraph 1 of article 1 of Law no. 5/2022 11 January.

2.3. The Reporting Persons shall only provide such specific and objective information that is required to determine whether the object of their Disclosure falls within the scope described. They must also refrain, unless this is essential to understand the scope of the Disclosure, from providing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sex life or sexual orientation of the Parties concerned, the Reported party or any other natural person.

2.4. Information: The Reporting Person shall receive an acknowledgement of receipt within a maximum of seven (7) days from receipt of the disclosure in the Ethics Channel and be informed by Glovo, in a clear and accessible manner, of the requirements, competent authorities and form and admissibility of the external complaint.

2.5. Precedence between internal means of reporting and public

disclosure: the Reporting Person can only resort to external reporting channels when:

(i) There is no internal reporting channel;

(ii) The internal whistleblowing channel only admits the filing of complaints by workers;

(iii) Has reasonable grounds to believe that the breach cannot be effectively known or resolved internally or that there is a risk of retaliation;

(iv) Has initially lodged an internal complaint without being notified of the measures envisaged or adopted following the complaint within the time limits; or

(v) The infraction constitutes a crime or administrative offence punishable by a more than 50,000 (euro) fine.

The Reporting Person may only publicly disclose an infringement when:

(i) Has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest, that the breach cannot be effectively discovered or resolved by the competent authorities, given the specific circumstances of the case, or that there is a risk of retaliation even in the case of an external complaint; or

(ii) Has filed an internal and external complaint, or directly an external complaint under the terms provided for in this law, without adequate measures being adopted within the legal deadlines.

The person who, apart from the cases provided for in the previous number, makes a media organization or journalist aware of an infringement does not benefit from the protection conferred by the law, without prejudice to the applicable rules regarding journalistic secrecy and protection of sources.

The provisions of the Portuguese Whistleblower Protection Act do not affect the obligation to report provided for in Article 242 of the Code of Criminal Procedure.

2.6. The Reporting Person may request, at any time, that Glovo communicates the result of the analysis carried out on Disclosure within 15 days after the respective conclusion.

3. Record keeping of the Disclosures

3.1. Records of every Disclosure received shall be stored for 5 (five) years and, regardless of this period, during the pendency of judicial or administrative proceedings related to the Disclosure.

3.2. Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

---

[1] Section 7, Definition of "Breach"