Glovo

For Public Use

Information Security Policy

Version 1.0 - Valid from [November 2026]

INDEX

1. Purpose 3
2. Scope 3
3. Our Commitment 3
4. Principals 3
5. Information security objectives 4
6. Policy framework 4
7. Roles and responsibilities 4
8. Compliance and review 4
9. Contact and reporting 5

1. Purpose

Information is an essential asset for Glovo, its customers, couriers, commercial partners, suppliers and other stakeholders. This policy sets out Glovo's commitment to protecting the information it processes and to operating its services securely, reliably and in line with legal, contractual and regulatory obligations.

2. Scope

This policy applies to GlovoApp23, S.L. and its subsidiaries ("Glovo"), its employees and contractors, and the third parties that process information on its behalf.
Glovo's Information Security Management System (ISMS) certified against ISO/IEC 27001:2022 covers the management, operation, maintenance and support of the GlovoApp23 on-demand platform, which connects businesses, including restaurants, with riders when an order is placed, in accordance with the current Statement of Applicability.

3. Our Commitment

Top Management approves this policy and is committed to:

- protecting the confidentiality, integrity and availability of information;
- meeting applicable legal, regulatory and contractual requirements, including data protection law;
- providing the resources needed to run and improve the ISMS;
- continually improving the ISMS and its controls.

4. Principals

The previous commitment is based on the following mandatory basic principles:

- **Risk-based security**: we assess the risks to information and apply proportionate controls to reduce them to an acceptable level.
- **Protection of data**: we identify sensitive data, including personal and payment data, and protect it with technical and organisational measures such as encryption and access control.
- **Least privilege:** access to information and systems is granted only when needed for a person's role and is reviewed regularly.
- **Secure by design**: security and privacy requirements are built into our products, features and systems from the start.

- **Resilience:** we prepare for incidents and disruptions so that critical services continue and recover quickly.
- **Lawful processing:** personal data is processed lawfully, fairly, transparently and only for the stated purposes.
- **Third parties**: suppliers and data processors must meet confidentiality, security and data protection obligations appropriate to the information they handle.
- **People**: everyone who handles information on Glovo's behalf receives awareness training and knows their responsibilities.
- **Continuous Improvement**: Orient towards continuous improvement of the Information Security Management System and associated controls based on the established ISO 27001:2022 and affected regulations.

5. Information security objectives

This policy is the framework for Glovo's information security objectives. Objectives are measurable, have an owner and a target date, and are reviewed at least once a year by Top Management.

6. Policy framework

This policy is supported by internal policies and procedures covering, among other topics: acceptable use, access management, asset management, cryptography, data classification, secure development, change management, vulnerability and patch management, logging and monitoring, network and cloud security, physical security, backup, business continuity, incident management and third-party risk management.

7. Roles and responsibilities

Top Management is accountable for the ISMS. The Information Security team defines, operates and monitors the ISMS. Every employee, contractor and third party with access to Glovo information must follow this policy and report suspected security incidents without delay.

8. Compliance and review

Compliance with this policy is checked through internal audits, monitoring and management reviews. Breaches of this policy may lead to disciplinary or contractual measures. This policy is reviewed at least once a year and whenever significant changes occur.

9. Contact and reporting

- Security questions from partners, customers or suppliers: Contacts
- Privacy questions: Glovo Privacy Policy

