2.3. **Ethics** and compliance

Ethical conduct and compliance with all market regulations within Prosegur's footprint are critical to the group's business strategy. Thus, aspects such as frequent exposure of employees to risk situations, the duty to protect customers and society, and management of large sums of money and personal goods all require responsible oversight and the highest standards of integrity.

Which is why Prosegur has a Corporate Compliance Programme in place, which establishes control measures designed to prevent and duly manage risks associated with breaches of regulations in each market where it operates. This programme addresses all the related legal matters and, in particular, those regarding money laundering, competition law, crime prevention and compliance with securities market regulations.

Corporate Compliance Programme

Responsibility for supervising the programme lies with the Compliance Committee, made up of management representatives from the Legal, Finance, Human Resources, Risk Management, Internal Audit and Compliance divisions, which acts independently and report to the Audit Committee. To ensure that the responsibilities entrusted to the Committee are effectively implemented, a compliance officer has been designated in each market within the group's footprint, who assures observance of applicable ethical principles and local regulations.

During 2018 Prosegur implemented a series of measures as part of the Corporate Compliance Programme, which necessarily included improvements in the fields of data protection due to the introduction of the new General Data Protection Regulation (GDPR), a European directive aimed at safeguarding the data of individuals via a focus on personal data processing and free circulation of such data. The group adapted to said directive as follows.

Adaptation to General Data Protection Regulation (GDPR)

During 2018, Prosegur Cash implemented a series of measures as part of the Corporate Compliance Programme, which necessarily included improvements in the fields of data protection due to the introduction of the new General Data Protection Regulation (GDPR), a European directive aimed at safeguarding the data of individuals via a focus on personal data processing and free circulation of such data. The group adapted to this directive as follows:

1. Record of processing activities

2. Risk level assessment

3. Impact assessments

4. Implementation of measures derived from risk analysis

5. Employee training and awareness

6. Maintenance and continuous improvement of the risk management system

Data protection went from being the exclusive responsibility of technical teams to be the responsibility of all individuals at the organisation. New aspects introduced by the recent legislation include the following:

LEGAL MEASURES

- Update of data protection clauses provided to the third parties
- Legal ground for processing data
- Implementation of mechanisms for obtaining the consent data subjects to the processing or disclosure of their data
- Elaboration of contracts adapted to the European Regulation
- Privacy impact assessment

ORGANISATIONAL MEASURES

- Designation of a Data Protection Officer responsible for monitoring compliance with the law
- Creation of data breaches notification procedure adapted to GDPR
- Updating data subject access request procedures, including the right to data portability

TECHNOLOGICAL MASURES

- Security procedures
- Logical security
- Physical security
- Cryptography
- Development and maintenance of information systems
- Operation of systems
- Anonymization
- Pseudonymization

Legal and organisational measures have been introduced by Prosegur to comply with the new regulatory requirements, as well as 394 technological measures. Among the first of these, the creation of the Data Protection Committee particularly stands out. This committee contains representatives from the businesses and corporate areas, acting as Functional Data Processing Controllers under the supervision of the Data Protection Officer (DPO).

Its actions are guided by the GDPR Governance Model for which the Board of Directors has maximum responsibility and that is divided into three lines of defence: those comprised by the Data Protection Committee, the Privacy and Data Protection Supervisors and Officers Committee, and finally, the third line of defence, that represented by Internal Audit.

Risk approach

End-to-End Data Protection Management Model

One new development in 2018 that reaches beyond the demands of the GDPR is a Strategic Plan for Information Security. This involved deployment of an Information Security Governance Model based on three lines of defence. A series of indicators and metrics were also established to provide Prosegur with information on the security status of information across all of its businesses. This ensures that best practices can be incorporated in step with the company's strategic development:

1st Line of Defence

Implementation of operating security at the company

2nd Line of Defence

Independent security strategy and framework

3rd Line of Defence

Security standard compliance and framework tests (audit)

Code of Ethics and Conduct

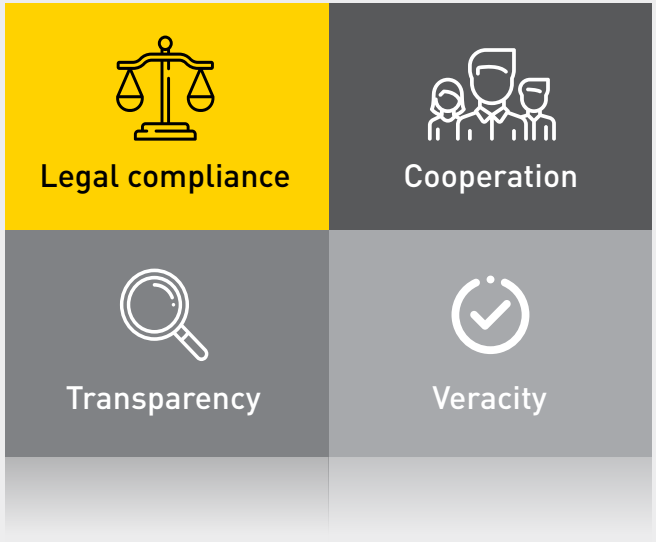
Prosegur has in place a Code of Ethics and Conduct, which was approved by the Board of Directors on 26 April 2017. The Code sets out guidelines for the standards of conduct and sound practice for all Prosegur professionals as they go about their duties, as well as in their relations with third parties. The Code is binding and mandatory for all company governing bodies, executives and employees. Furthermore, it regulates all conduct and relations between said groups and with external groups.

Disciplinary measures have been established for those breaching the provisions of the code, following an investigation conducted by a team of impartial experts headed up by the Compliance area, which will propose the appropriate corrective measures.

The Code of Ethics and Conduct can be found at the corporate website and is provided to each employee when joining the company. In 2018 a total of 5,193 employees underwent training in the Code of Ethics and Conduct.

Seeking to partner with other international companies to support ethics and integrity, Prosegur is a signatory and proponent of the "Code of Conduct and Ethics" of the International Security Ligue and recognises the "Code of Conduct and Ethics for the private security sector" from the Confederation of European Security Services (CoESS).

Pillars of the Code of Ethics and Conduct



Whistleblowing Channel

Prosegur has a Whistleblower Channel available to enable any person, regardless of whether they form part of the group or not, to report any conduct that may contravene the Code of Ethics and Conduct, as well any potential human rights violations, illicit behaviour, and any financial and accounting irregularities. This channel can be accessed by going to the corporate website and completing the form available there.

The Internal Audit Division confidentially reviews all the submitted reports and forwards them, as appropriate, depending on their type and severity, to the division responsible for their due response, investigation and resolution. Based on conclusions drawn from the investigations, appropriate measures will be adopted at Audit Committee meetings when company intervention is required.

During 2018 a total of 18 violations of the Code of Ethics and Conduct were reported via the channel.

17 PARTNERSHIPS FOR THE GOALS

Seeking to promote sector development, improve quality standards and drive more advanced public policies to support sustainable development, Prosegur engages in industry dialogue via memberships of associations and organisations. The main international organisations to which the company is adhered include the International Security Ligue, the Confederation of European Security Services (CoESS), the European Security Transport Association (ESTA), the Asian Cash Management Association (ACMA), the ATM Industry Association (ATMIA), the Aviation Security Services Association – International (ASSA-I) and United Nations Global Compact. Likewise, at the local level Prosegur is adhered to leading industry organisations in countries within its footprint.

2.3.1. Due diligence with regard to human rights

Prosegur diligently complies with its duty to foster respect for human rights as an inalienable aspect of its activities. The company channels resources and effort into enshrining respect for the rights listed in the Universal Declaration of Human Rights (UDHR), adopted by the UN General Assembly, within its practices and procedures, as well as the recommendations of the United Nations Global Compact, of which it is a signatory since 2002.

This commitment goes beyond compliance with the laws and regulations of the territories in which Prosegur operates, and, in particular, offers a stronger protection framework in countries where the state's ability to safeguard human rights is limited. For several years now, the company has been working with a view to adopting the principle of due diligence to define the internal control elements necessary to optimise the management of this matter and, with it, to be able to state that everything possible is done to encourage good practice and to prevent, detect and eradicate irregularities in the area of human rights.

Likewise, within the framework of the Prosegur management system, formal policies and procedures have been established to prevent and mitigate potential human rights violations. This system forms part of the organisation's global risk management, for which reason the critical risks are identified, and the management of them is assessed and supervised through a set of key indicators in each market. Depending on the type of risk and its relevance, appropriate procedures are established to prevent, detect, avoid, mitigate, offset or share the effects of its possible materialisation.

Risk management and control system | **Whistleblowing channel** | **Human Rights due diligence processes** | **Training**

Other Human Rights policies and procedures:

- Corporate Responsibility Policy
- Prosegur Cash Code of Ethics and Conduct
- Occupational Health & Safety Policy
- 3P HR Decalogue
- 3P Security and Associated Policies Decalogue
- 3P General Procedure for Reporting

Prevention and control measures

POLICY FRAMEWORK:

Various policies and procedures combine to serve as the first barrier of prevention and control in human rights matters: Code of Ethics and Conduct, Corporate Responsibility Policy, Discrimination and Harassment Complaints Procedure, Whistleblowing Channel Procedure, Health and Safety Policy, among others.

WHISTLEBLOWING CHANNEL:

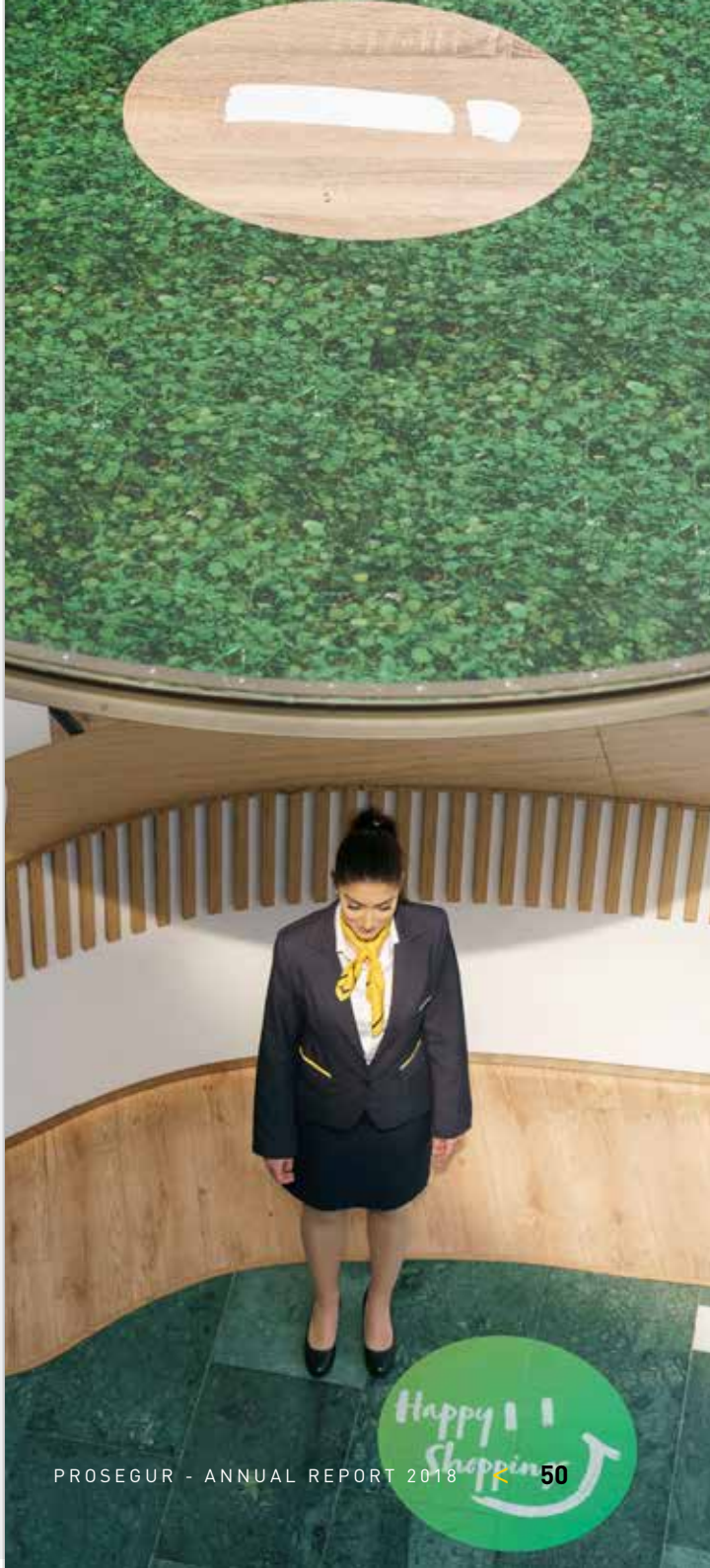
Through this method, the company enables employees and third parties to report any human rights violations that may arise, in a confidential and anonymous manner. During 2018 Prosegur received no reports of any human rights violations via its Whistleblowing Channel.

SUPERVISION:

The supervision of human rights matters is based around a solid structure. The Audit Committee of the Board of Directors is responsible for reviewing any related matter through periodic reports.

SPECIFIC TRAINING:

Human rights are integrated into the various training courses carried out from the areas of Human Resources and Compliance. In addition, mandatory training plans for operating staff include sessions on critical issues such as the use of force, gender violence, cultural diversity and human rights in the company.



Seeking to maintain an efficient focus on human rights management, in 2018 Prosegur introduced a due diligence process, additional to those already in place, with the following aims:

Goal I:	**Identifying and prioritising** risks related to human rights.
Goal II:	**Review of** policies and procedures for human rights management, with a corporate and local focus.
Goal III:	**Identifying opportunities to improve** both prevention and mitigation.

The project, which was implemented by a prestigious third party, adhered to leading international directives and documents in the field. Additionally, an analysis was made by a specialist independent consultancy of the human rights impact on the company activity, defining the degree of connection with each matter, its possible internal and external causes and the potential effect. Throughout this process, improvement opportunities were identified that were associated with the management of risk prevention and/or control mechanisms found in the implementation process.