



Code of Conduct for Global Security

**Renault
Group**

01	Introduction	
	<ul style="list-style-type: none">• Why a Code of Conduct ?• Purpose of the code• Global Security	<u>4</u> <u>4</u> <u>4</u>
02	Scope	
	<ul style="list-style-type: none">• Scope• Employees concerned	<u>6</u> <u>6</u>
03	Principles and expectations	
	<ul style="list-style-type: none">• Fundamental principles and scenarios	<u>8</u>
04	Reference Documents and whistleblowing alert system	
	<ul style="list-style-type: none">• Reference Documents• Whistleblowing alert system• Responsible of the Code within Renault Group	<u>18</u> <u>18</u> <u>19</u>

01 Introduction



01 Introduction

WHY A CODE OF CONDUCT?

Certain documents, such as the **Code of Ethics** and the **Anti-Corruption Code of Conduct**, are intended for all employees of Renault Group and its controlled subsidiaries: managers, employees, apprentices and temporary workers. Those who work directly or indirectly with Renault Group are invited to consult and refer to them.

The Code of Ethics not only sets out principles and commitments, but above all defines the state of mind in which internal and external professional relations should be approached. It also sets out the behaviour to be adopted in the event of breach of ethics.

The Anti-Corruption Code of Conduct is a decision-making tool on which each and every one can rely. In this sense :

- It defines corruption, presents its form and risks through examples (conflict of interests, gifts or invitations, etc.) and lists the most common warning signs;
- It sets out the behaviour to adopt and the rules to respect in order to prevent corruption and remedy it if necessary;
- It refers to detailed procedures in case of doubt.

The Group's Code of Ethics and Anti-Corruption Code of Conduct are complemented by dedicated codes of conduct. Their purpose is to define the ethical rules governing the practice of a profession, function or activity for which higher ethical standards are required.

PURPOSE OF THE CODE

The **code of conduct for global security** is part of this framework.

This code sets out the guiding principles that apply when it comes to Global Security.

GLOBAL SECURITY

Global Security covers all measures aimed at preventing and protecting individuals and Renault Group's tangible and intangible assets and its subsidiaries against accidental damage and malicious acts. It also includes monitoring, crisis management and business continuity measures.

For the purposes of this code:

- **Security** covers all the measures (technical, human and organizational) deployed to prevent and detect human malicious acts, and to intervene where necessary.
- **Industrial security** covers all the measures (technical, human and organizational) deployed to prevent and detect industrial incidents, protect people and property from their consequences, and intervene where necessary.
- **Private security** refers to all activities and services provided by private companies or security guards, with the aim of protecting property, people or events.

Renault group's Code of Ethics and Anti-Corruption Code of Conduct can be consulted on the Ethics and Compliance Intranet / see « *Ethical standards* » (accessible from the Declic home page) and the web site renault.com/see « *commitments* ».

02

Scope



02 Scope

SCOPE

The code of conduct for global security applies to all Renault Group legal entities, subsidiaries and service providers.

This code of conduct does not apply to individuals performing health and safety activities related to operations. These activities fall within the scope of the Health, Safety & Environment Department.

EMPLOYEES CONCERNED

The **code of conduct for global security** is intended for all managers and employees involved with the "Prevention and Protection" function of Renault Group and its subsidiaries, whether they are hierarchically or functionally attached to the Group Prevention and Protection Department (D2P)*.

These include the Reception, Prevention and Protection (A2P)** services for sites and affiliates in each country.

This code is also intended for any person who, in the course of his or her duties, is involved on a permanent or occasional basis in the area of Global Security (site director, HR, procurement etc.)

(*) **D2P** : Prevention & Protection Department, responsible for defining the Prevention and Protection policy at the Group, Country or Business Unit level.

(**) **A2P** : Reception, Prevention & Protection Department, in charge of covering malicious acts and industrial risks for one or more sites.

03

Principles and expectations

03 Principles and expectations

FUNDAMENTAL PRINCIPLES AND SCENARIOS

Any person who, by virtue of their duties, acts on behalf of Global Security, is a contributor and therefore a guarantor of the respect and implementation of the Renault Group Code of Ethics through their behavior. Such persons must pay particular attention to ensuring strict compliance with the principles defined below.

► Principle 1 : Comply with the law

Any person who, by virtue of their duties, acts on behalf of Global Security, undertakes to know and comply with the regulations applicable to their missions, as well as Renault Group rules and procedures. Tools must be deployed and used in accordance with regulations in force. Any recording, control or monitoring process or device must comply with the law.

Scenario 1

You're an A2P (Reception, Prevention and Protection) manager for a tertiary site. For several months, you have been receiving reports regarding the disappearance of computer equipment. You are convinced that one of your employees is involved and you ask that said employee for their access authorisations to be revoked and that you be given permission to search their locker. While waiting for approval from management, you set up targeted monitoring of the person in question (webcam and telephone recording).

What should you do?

It is strictly prohibited to question the integrity of an employee in the absence of evidence or facts. An accusation directed against a person that is likely to result in judicial, administrative or disciplinary sanctions that are based solely on suspicion constitute misconduct. Moreover, it is not possible to remove access without having followed internal procedures, and in particular disciplinary procedures. If misconduct is suspected, the matter should be referred to management and the relevant HR department.

How can this scenario be avoided?

Respect for individual freedoms and the presumption of innocence must guide your day-to-day actions. When in doubt, always seek the support of your ethics and compliance correspondent. Your hierarchical manager, social relations manager and/or site director are also natural supports and should be consulted.

03 Principles and expectations

► Principle 2: Set an example

Any person who, by virtue of his or her functions, is involved in Global Security, undertakes to behave in an exemplary manner in all circumstances. They contribute to the development of a culture of integrity and ethics within Renault Group, in accordance with the Code of Ethics.

Through their behavior, they contribute to the development of constructive and positive relations with the other Renault Group departments with which they are in contact.

Scenario 2

You are a member of the Management Committee of a tertiary site. You are expecting a delegation from one of your strategic partners. The visitors are running late, and your schedule will be difficult to keep. The delegation arrives at the reception desk. You order the A2P (Reception, Prevention and Protection) agent to not carry out the visitor control formalities, claiming that you know the visitors very well and that you can vouch for their integrity. The A2P agent asks you to wait while they speak to their supervisor. As you are already behind schedule and are annoyed by the agent's attitude, you bypass access control and invite your delegation to enter the site.

❑ What should you do?

Safety measures contribute to everyone's safety. They can sometimes be perceived as burdensome. However, they are essential to the safety of the Group and its employees. Each employee has an obligation to respect the security policy and to promote it through exemplary behavior. It is imperative to remind all employees that through our behavior and by setting an example, we contribute to the safety of Renault Group. Violating safety rules can lead to disciplinary proceedings.

❑ How can this scenario be avoided?

Management must ensure that the rules are clearly understood by all those involved. Compliance with these rules contributes to the overall security of the site and the site's employees. The site manager helps to ensure that these rules are applied by everyone, in all circumstances, both verbally and in writing. Any derogations cannot be decreed. They are subject to validation. Visitor registration formalities can be anticipated to reduce waiting time.

03 Principles and expectations

▶ Principle 3: Respect individuals

Any person who, by virtue of his or her functions, plays a part in Global Security undertakes to exercise his or her responsibilities in a manner that respects individuals. When, in the performance of his or her duties, a Global Security officer is unable to resolve a dispute consensually with a person who refuses to undergo the verifications and controls required by law, he or she must report immediately to the person identified for this purpose, who will then decide whether or not to call the appropriate law enforcement authorities.

Scenario 3

An employee arrives in a company vehicle at the site's "vehicle" exit. The checkpoint supervisor asks his agent to visually check the interior of the vehicle. A significant number of items clearly belonging to the company are visible in the trunk. The employee is unable to provide proof and admits that he intended to steal the items. The checkpoint supervisor apprehends the employee and detains him for 3 hours as a sanction.

❑ What should you do?

The checkpoint supervisor cannot impose sanctions on the employee. In this case, his role is to make a formal observation and report back. Management and the relevant HR department should be informed immediately in this context, in order to initiate disciplinary proceedings against the employee. He or she must not be subjected to any violence, humiliation or treatment contrary to human dignity.

❑ How can this scenario be avoided?

The A2P (Reception, Prevention and Protection) coordinator must ensure, through regular checks and instructions, that A2P agents are fully aware of the scope of their actions, and that they always act with strict respect for people and internal rules.

03 Principles and expectations

► Principle 4: Demonstrate integrity

Any person who, by virtue of his or her functions, is involved in Global Security, works in the sole interest of Renault Group. In particular, they must comply with the Renault Group's Anti-Corruption Code of Conduct and must not derive any direct or indirect personal benefit of any kind whatsoever from the performance of their duties. Any act of corruption (active or passive) or facilitation payment is strictly forbidden in all countries. No one should use their relationship with the authorities illegally, inappropriately or for personal gain, especially if this relationship is linked to a past activity that may have conferred other prerogatives (e.g. retired police officer).

Scenario 4

At the last steering committee meeting preceding a call for tenders, the company providing Security services gave purchase vouchers and invitations to shows to the entire Prevention and Protection team of the site, as a thank-you for the working relationships built up over the years.

What should you do?

Renault Group sets limits and a context for gifts, invitations or benefits of any kind, whether solicited, received, offered or given, directly or indirectly. Gifts or invitations, provided they comply strictly with the rules of courtesy and are of modest and measured value, are tolerated as long as they cannot influence a decision or a business relationship. However, you must obtain the prior and written authorization of your hierarchical superior. For further information: please refer to the Gifts, invitations and business meals procedure available on the Ethics and Compliance intranet site, accessible from the Declic home page.

How can this scenario be avoided?

Communicate to companies working with Renault Group the Anti-Corruption Code of Conduct and the procedure for gifts, invitations and business meals, which they must respect.

03 Principles and expectations

► Principle 5: Respect the rules of confidentiality

Any person involved in Global Security, by virtue of their functions, is bound by a strict duty of confidentiality. They must implement appropriate measures to protect the confidential information they hold, communicate or receive. Any private use of confidential or personal information is strictly forbidden in accordance with the Renault Group Code of Ethics and the information protection policy in force.

Any person who, by virtue of his or her functions, is involved in Global Security, complies with the internal laws and regulations applicable in terms of personal data protection and respect of privacy.

Scenario 5

An A2P (Reception, Prevention, Protection) agent recounts around him the incredible circumstances in which an employee was checked with a ream of paper as he left the establishment. The agent enjoys telling this story, which always elicits interest and laughter from the audience.

What should you do?

The circumstances surrounding a security event are confidential information. They can only be discussed with management, as part of a disciplinary procedure or in the context of a court procedure. Disciplinary action must be taken against this type of behaviour.

How can this scenario be avoided?

The A2P (Reception, Prevention and Protection) coordinator of the site must ensure through regular checks and instructions, that A2P agents are fully aware of the scope of their actions, and that they always act in such a way as to strictly maintain the confidentiality of information.

03 Principles and expectations

► Principle 6: Do not claim to be a representative of public authority

The employees or service providers who work for Global Security are not public officials and do not represent them. Therefore, any person who, by virtue of his or her functions, is involved in Global Security, shall refrain from causing any confusion with themselves and the forces of law and order, particularly through his or her behavior, mode of communication or words. They may not purport to be carrying out any missions on behalf of public administrative authorities or have been given any powers by any public administrative authorities which have not been entrusted them by said authorities.

Scenario 6

During a random bag search by the site's A2P (Reception, Prevention, Protection) department, an employee refuses to submit to the search. The agent claims that having been a member of the police force, he or she is authorized to carry out the search.

❑ What should you do?

Bag searches are not allowed, only a visual inspection is allowed. Personal belongings may only be touched with the prior authorization of the person concerned. As the person concerned must give his or her consent, he or she has the right to object to the search. He or she may also require the presence of a witness. In the event of suspected theft, the security manager or the director of the establishment or subsidiary may call upon a judicial police officer who has broader powers.

❑ How can this scenario be avoided?

The A2P (Reception, Prevention and Protection) coordinator of the site must ensure through regular instructions and controls, that security guards are fully aware of the scope of their actions, and that they always act in strict compliance with local regulations. Employees should also be made aware of the consequences of refusing to show the contents of their bag.

03 Principles and expectations

▶ Principle 7: Facilitate controls, audits, and judicial procedures

Any person who, by virtue of his or her functions, intervenes in Global Security, must assist in the controls carried out by administrations, authorities and authorized bodies. In compliance with legal and regulatory provisions relating to the protection of privacy, they must allow the consultation and/or communication, as quickly as possible, of any document officially requested.

Scenario 7

A law enforcement officer requests numerical data relating to the "access control" system in the absence of any official request from the authorities. This information constitutes personal data, which is protected.

❑ What should you do?

Refuse the request unless a formal request is provided. Inform the officer that the information requested is protected personal data. In addition, notify the A2P (Reception, Prevention Protection) coordinator that the request has been made.

❑ How can this scenario be avoided?

Inform the authorities that this information is protected and cannot be shared unless a request made in accordance with regulations (judicial requisition).

▶ Principle 8: Develop and maintain your skills

Any person who, by virtue of his or her functions, is involved in Global Security, undertakes to act with professionalism and to ensure that he or she acquires and maintains his or her skills through any training required by national and/or international regulations.

Scenario 8

You work on a tertiary site. You have been trained and appointed to be in charge of evacuating your department, but your recollection of your training and the date of your last exercise is hazy. Moreover, you have very little time to devote to this function, especially as there has never been an evacuation alarm since you took over.

❑ What should you do?

The "Evacuation Officer" function is a key component of the alarm system. It must not be improvised and approximated. If you are in doubt about your role as "Evacuation Officer", you should contact the A2P (Reception, Prevention Protection) coordinator at your site and request new training. You ensure that your department's employees are familiar with the evacuation rules related to their duty stations.

❑ How can this scenario be avoided?

The A2P (Reception, Prevention Protection) coordinator of the site schedules and conducts exercises and training in accordance with current regulations and internal rules. He keeps a list of evacuation officers to be retrained and takes care of their training. The function of "evacuation officer" is an official function that is subject to appointment.

03 Principles and expectations

► Principle 9: Respect current instructions

Any person who, by virtue of his or her functions, intervenes in Global Security, carries out his or her missions in transparency with his or her superiors by developing a relationship of trust. The procedures and systems put in place are based on the Renault Group Safety Management System (available on the Intranet) and are reported to the competent persons.

Scenario 9

You are a member of the A2P (Reception, Prevention Protection) team at a production site, and you are on standby at the CSS (Central Security Station). When you take up your position, you learn that the P04 fire detector periodically activates an alarm. A maintenance technician is scheduled to restore it the following day. It's 1 a.m. and the fire alarm goes off. The alarm register shows that it was detector P04. You acknowledge the alarm and isolate detector P04. You note in the log that detector P04 is out of order and that its replacement is planned.

What should you do?

In accordance with the Renault Group's "Prevention and Protection" guidelines (SMS: Safety Management System), patrols "to dispel doubts" are part of the alarm management system. Doubts about the availability of detection equipment must not, in themselves, justify not carrying out patrols "to dispel doubts".

How can this scenario be avoided?

The A2P (Reception, Prevention and Protection) coordinator of the site must ensure that all employees under his or her responsibility understand the rules applicable to their activities. Skills and knowledge checks must be carried out regularly and adapted as necessary. In addition, the A2P coordinator must ensure that all detection and alarm systems are fully operational. In the event of operational unavailability, he or she must put in place temporary corrective measures to ensure the proper functioning of his or her security organisation.

03 Principles and expectations

▶ Principle 10: Remain impartial

Any person who, by virtue of his or her functions, intervenes in Global Security, shall perform his or her duties with the utmost impartiality, basing his or her analysis on arguments. They shall refrain from allowing their personal opinions to prevail, and refrain from any bias, prejudice, favoritism or discrimination.

Scenario 10

You have issued a call for tenders for guarding services and selected the company where your brother works as Director of Operations.

What should you do?

Even if you believe you are acting for the good of the company, your personal connection constitutes a conflict of interest. Before selecting suppliers from the panel, you must notify your manager and your RGP (Renault Group Procurement) correspondent. Your manager must analyse the reality of the situation and exclude you from the decision-making process.

How can this scenario be avoided?

Read and apply the [Conflicts of Interest Management Procedure](#) available on the Ethics and Compliance intranet site, at the bottom of the Declic home page.

Inform your manager in advance by submitting a spontaneous declaration of conflict of interest. With the help of the ethics and compliance correspondent and, if necessary, human resources, he or she will analyse the situation, take the necessary decision and formalise it. If in doubt, you should make a spontaneous declaration of conflict of interest. Anyone can find themselves in a conflict of interest situation, but not declaring it is reprehensible.

04

Reference Documents and whistleblowing alert system



04 Reference Documents and whistleblowing alert system

REFERENCE DOCUMENTS

- ▶ All legal texts relating to private security legislation in force in each country.
- ▶ Ethics and compliance standards.
- ▶ All documents relating to the Security Management System.
- ▶ The procedure Ensuring the regulatory oversight of Prevention and Protection ([RPIFSECUR20140019](#)).

WHISTLEBLOWING ALERT SYSTEM

Any person listed below can submit an alert in complete confidentiality through the Renault Group whistleblowing system.

This system is accessible to all employees, former employees, unsuccessful candidates from recruitment, shareholders, partners and holders of voting rights, members of the administrative, management or supervisory body of one of the Renault Group entities, external and occasional employees (temporary staff, trainees, apprentices and employees on assignment etc.), co-contractors (e.g., dealers or suppliers/service providers) and their sub-contractors. It complements the channels for reporting alerts, which include management, human resources, employee representatives, the Ethics and Compliance Department and the Deputy Department of Professional Alerts.

▶ Conditions for acquisition of the whistleblower status

To qualify for whistleblower status, a number of criteria must be met:

1. Be a natural person. Report or disclose facts that have occurred or are very likely to occur that are contrary to the law, the Code of Ethics, the Anti-Corruption Code of Conduct or this Code;
2. act without direct financial consideration and in good faith;
3. obtain the information in the course of their professional activities. If the information was not obtained in the course of professional activities, the person reporting it must have had personal knowledge of it.

▶ Access to the whistleblowing system

The whistleblowing system is accessible on the Ethics and Compliance Intranet / « *Whistleblowing* » section (accessible from the bottom of the Declic home page) and on the [renault.com](#) website / Commitments / Ethics section or by flashing the QR Code :



04 Reference Documents and whistleblowing alert system

► Protection for the whistleblower

Renault Group guarantees the strict confidentiality of the identity of the whistleblower, the person who is the subject of the alert and the facts that are the subject of the report. Alerts are treated confidentially, subject to applicable legal obligations and possible judicial proceedings. Whistleblowers also benefit, where applicable, from civil and criminal immunity as well as protection against the risks of retaliation and discrimination.

No disciplinary or discriminatory measures may be taken against employees who have made a report, even if the facts are not proven, provided that these employees have acted in accordance with the criteria set out above. However, the abusive, malicious use of this system or its use in bad faith may result in disciplinary sanctions and legal proceedings.

RESPONSIBLE OF THE CODE WITHIN RENAULT GROUP

The Prevention and Protection Vice President is the “owner” of the Code of Conduct for Global Security. He or she is responsible for modifying and updating it.

If you have any questions or require information about the Code of Conduct for Global Security, please contact him or her.

