

# Code of conduct for Software & Digital



**Renault  
Group**

## 01

### Introduction

- Why a Code of conduct ? [4](#)
- Purpose of the Code [4](#)

## 02

### Scope of the Code

- Scope [8](#)
- Employees concerned [8](#)

## 03

### Principles and expectations

- Cybersecurity [10](#)
- Protection of personal data [15](#)
- Artificial intelligence [19](#)
- Responsible Digital [23](#)

## 04

### Reference documents and whistleblowing

- Reference documents [28](#)
- Whistleblowing alert system [29](#)

# 01 Introduction



# 01 Introduction

## WHY A CODE OF CONDUCT?

Some 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. All those who work directly or indirectly with Renault Group are invited to consult them and refer to them.

The **Code of Ethics** not only lays down principles and specifies commitments, but above all it defines the state of mind in which internal and external professional relations should be approached. It also sets out the behaviours to adopt in the event of a 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 forms and risks through examples (conflict of interest, gifts or invitations, etc.) and lists the most common warning signs;
- it sets out the behaviour to adopt and the rules to comply with 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 business, function or activity for which higher ethical standards are required.

## PURPOSE OF THE CODE

The **Code of Conduct dedicated for IT & Digital Services** is part of this framework.

It establishes all the principles that apply to **our business line as IT specialists** and sets out the rules and behaviour that **each of us must respect, in the following 4 areas:**

### 1.1. CYBERSECURITY

Changes in digital usage and the development of new, increasingly connected products mean that people are more exposed to cyber-attacks. In order to protect our customers, maintain their trust and comply with the relevant regulations (in particular the NIS 2 directive, UN regulation 155 and specific regulations incorporating cybersecurity requirements such as the AI Act), we are strengthening the company's cybersecurity at all levels.

For Renault Group's cybersecurity to be effective, all employees have a duty to respect Renault Group's Cybersecurity Policy and cybersecurity rules and to act with vigilance. As IT specialists, we must also act in accordance with the ethical principles set out in this code.

Renault group's Code of Ethics and Anti-Corruption Code of Conduct can be consulted on the Ethics and Compliance Intranet / see « *Our standards* » (accessible from the Declic home page) and the web site [renaultgroup.com](http://renaultgroup.com)/see « *Responsibility/Ethics* ».

# 01 Introduction

## 1.2. PROTECTION OF PERSONAL DATA

In its Personal Data Protection Policy, Renault Group considers that compliance with the relevant regulations is an opportunity to strengthen the trust of its stakeholders (shareholders, customers, suppliers and employees).

As trust is a value to which Renault Group is committed, the protection of personal data is one of our ethical references in the conduct of our activities.

In particular, Renault Group intends to ensure the greatest possible transparency in the processing of personal data provided by its customers or collected through its various contacts.

Renault Group employees are essential to this policy. They receive training on the processes and daily support from specialised teams to ensure the protection of the personal data of customers, employees as well as representatives of our suppliers and partners.

As IT specialists, we are directly involved in data processing issues. We must therefore respect the principles and expectations set out in this Code of conduct.

## 1.3. ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is increasingly present in the various functions of our company, and its deployment is constantly expanding: from helping to summarise documents, to setting up Chatbots or creating algorithms to send the right customer offer, at the right time.

AI offers us many opportunities, but it can also present significant risks if it is misused, poorly designed or misunderstood: there is a reputational risk in the event of "hallucination" (a model that generates incorrect or inconsistent information) or misinterpretation when the AI-based conversational agent produces nonsense. There is also a risk of damage to the customer relationship if customer information is inadequately processed, whether during the sale, delivery or after-sales service. Finally, there are more serious risks, such as the vulnerability of driver assistance systems to attacks aimed at disrupting them.

Every user must respect certain rules when using AI. And as computer scientists, we have a role to play when we design or deploy AI. It is our responsibility to act in a way that is consistent with ethical principles and regulations such as the AI Act (European risk-based regulatory approach) in order to avoid any harmful impact. These principles are described in this Code of conduct.

# 01 Introduction

## 1.4. RESPONSIBLE DIGITAL

Renault Group is committed to integrating the principles of sustainable IT into its corporate culture in order to achieve its digital transformation while contributing to its environmental and social ambitions.

In 2022, Renault Group has therefore adopted a Responsible Digital approach. This is not just a trend, but a necessity driven by growing environmental impacts (energy and water consumption by Information Systems, consumption of rare metals and raw materials, etc.) and increasingly marked by regulations.

The aim of the Responsible Digital approach is to promote a more sober, conscious and inclusive use of digital technology in order to limit its environmental and social footprint within the Renault Group and for its customers. It is reflected in the rules and principles of deontology described in this code, which we, as IT specialists, must respect.

# 02 Scope



# 02 Scope

## SCOPE

The Code of Conduct dedicated for IT and Digital Services applies to all the legal entities of Renault Group and its subsidiaries.

## EMPLOYEES CONCERNED

The Code of Conduct dedicated for IT and Digital Services applies to all Renault Group employees and managers involved, on a permanent or occasional basis, in the development or maintenance of on-board software or off-board information systems.

# 03 Principles and expectations



# 03 Principles and expectations

## 3.1.1 CYBERSECURITY: GETTING INVOLVED

### Principle 1: Developing and maintaining your skills

All persons who, through their duties, are involved in IT projects, undertake to act with professionalism and to ensure that they acquire and maintain their cybersecurity skills through any training required in accordance with national and/or international regulations and internal rules.

#### Scenario 1

As IT Manager, you have received training in cybersecurity, but your memories of the training and the date of the last drill are distant. Moreover, you have very little time to devote to this training, especially as there has never been a cybersecurity incident since you took up your post.

#### ❑ What do you need to do?

The role of IT Manager is of particular importance in managing cybersecurity. If you have any doubts about your role in cybersecurity, you should contact your manager and ask for further training from the training school responsible for your area.

#### ❑ How can this scenario be avoided?

Although cybersecurity incidents may seem rare, it's important to remember that the consequences can be extremely high. It is imperative to remain vigilant and to participate regularly and actively in training courses to prevent any potential risks. Training schools programme and deliver training in accordance with the regulations and internal rules in force. They keep a list of critical cybersecurity functions in order to provide targeted training.

### Principle 2: Promoting cybersecurity

Any person who, through their duties, contributes to cybersecurity undertakes to promote cybersecurity among all employees.

#### Scenario 2

You are the Cybersecurity Correspondent. You are responsible for monitoring compliance in your entity/department and you have noticed that several IT staff are not properly following the cybersecurity rules and processes.

#### ❑ What do you need to do?

The Cybersecurity Correspondent is the Cybersecurity Department's point of contact within his or her area of responsibility. If certain IT teams have difficulty applying the rules and procedures, it is necessary to quickly launch a new awareness-raising campaign with these teams to re-motivate them on cybersecurity issues and remind them of the importance of the cybersecurity rules and processes.

#### ❑ How can this scenario be avoided?

Raising awareness should not be a one-off event. In order to maintain a high level of involvement from all the IT teams, it is absolutely essential that the Cybersecurity Correspondent ensures that these teams are regularly reminded and that their involvement is verified through drills (e.g. phishing tests).

# 03 Principles and expectations

## 3.1.2 CYBERSECURITY: RELYING ON ORGANISATION AND/OR GOVERNANCE

### Principle 3: Assessing cybersecurity risks

All persons who, through their duties, are involved in IT projects, undertake to work jointly with the cybersecurity teams in order to regularly identify, analyse and assess cybersecurity risks.

#### Scenario 3

You are appointed Product Leader for the development of a new IT solution. On initial analysis, you do not identify any cybersecurity risks associated with this solution, but a colleague tells you to take precautions nonetheless.

#### ❑ What should you do?

As Product Leader, you must ensure the cybersecurity of the product for which you are responsible. To do this, you need to work with the cybersecurity teams or your Cybersecurity Correspondent and cybersecurity experts to identify, analyse and assess the risks. This will provide you with the necessary information about the risks, enabling you to draw up and execute a risk mitigation plan to ensure that the product has the right level of cybersecurity.

#### ❑ How can this scenario be avoided?

The cybersecurity teams and Cybersecurity Correspondents work alongside all the project teams to ensure that cybersecurity is integrated into projects. As a Product Leader, you should contact them from the start of the project and work together throughout the life of the product (from design to decommissioning).

### Principle 4: Alerting to cyber-incidents and cyber-risks

Any person who, through their duties, is involved in IT projects, undertakes to alert the Security Operation Centre as quickly as possible to the existence or suspected existence of a cyber-incident or vulnerability in the information systems.

#### Scenario 4

You are a developer and during the testing of an IT solution, you realise that the solution being tested uses obsolete technology. Despite this, the solution seems to be working correctly.

#### ❑ What should you do?

Although the IT solution appears to be working correctly, the use of obsolete technology can make it vulnerable to attack. It is therefore important to inform the Security Operation Centre of this vulnerability so that it can analyse and check that it has not been exploited. At the same time, the Product Leader will ensure that the IT solution is updated, or failing that, that countermeasures are deployed to correct existing vulnerabilities.

#### ❑ How can this scenario be avoided?

The Product Leader must ensure that cyber-risks are reduced by making sure that product components are constantly updated, that product cyber-security tests are carried out by the project teams and by organising code, architecture and configuration audits and intrusion tests with the cyber-security teams. They must also work with the Security Operation Centre to set up real-time monitoring of product-related events, so as to detect incidents more quickly.

# 03 Principles and expectations

## 3.1.3 CYBERSECURITY : ACTING RESPONSIBLY

### Principle 5: Complying with the law and internal rules

All persons who, through their duties, are involved in IT projects must be familiar with and comply with the regulations applicable to their assignments as well as Renault Group rules and procedures. Tools must be developed, tested, deployed, updated, used and decommissioned in accordance with current regulations and internal rules relating to cybersecurity.

### Scenario 5

You are responsible for an application contributing to an information system. You are aware of a cybersecurity regulation, but you have doubts as to whether it applies to your application, as it is located outside the vehicle.

#### ❑ What should you do?

Cybersecurity law is constantly evolving. As a result, the Product Leader and IT specialists contributing to a project should always find out about the applicable regulations and their operational implications from the cybersecurity teams or their Cybersecurity Correspondent.

#### ❑ How can this scenario be avoided?

The cybersecurity teams have put in place a system of support for projects from the design stage through to decommissioning. Within this framework, the Product Leader must comply with a set of processes. The Product Leader will be supported in bringing and maintaining the project's compliance with the company's cybersecurity requirements, including compliance with applicable regulations.

# 03 Principles and expectations

## 3.1.3 CYBERSECURITY : ACTING RESPONSIBLY

### Principle 6: Identifying, controlling and securing assets

All persons who, through their duties, are involved in IT projects, undertake to implement, throughout the life of an IT product, all appropriate measures to control the cybersecurity risks duly identified during risk assessments.

### Scenario 6

As Product Leader, you have recently taken charge of a complex application under development. The project team is making rapid progress and you **will** soon be in a position to roll out the functions classified as MVP (Minimum Viable Product). But time is running out and you feel that you haven't fully mastered the cybersecurity of this complex application.

#### ❑ What should you do?

To control cybersecurity, you first need to ensure that all the assets involved in the operation of your application, and the interactions between them, are identified, listed and classified according to their criticality, taking into account the needs expressed by the Product Owner(s).

Thanks to your knowledge of your assets, you will be able, with the help of the cybersecurity teams or your Cybersecurity Correspondent, to identify, analyse and assess the vulnerabilities, threats and risks weighing on the application for which you are responsible. Depending on the risks identified and their level, you can then draw up a mitigation action plan in collaboration with the cybersecurity experts, and deploy the appropriate security measures to reduce these risks to a level that is acceptable to the company.

#### ❑ How can this scenario be avoided?

The cybersecurity teams have developed and deployed a risk management process that must be scrupulously respected by the Product Leaders. The Product Leader must initiate this process periodically, or when a product presents a major new vulnerability, suffers an incident or undergoes a major change that impacts cybersecurity requirements.

# 03 Principles and expectations

## 3.1.3 CYBERSECURITY : ACTING RESPONSIBLY

### Principle 7: Carrying out technical audits with respect for property, people and the environment

Any person who, through their duties, is involved in the preparation and/or performance of a technical audit, undertakes only to carry out actions authorised under an audit agreement. These actions must not be harmful to Renault Group, to any other natural or legal person (in particular its partners and customers), or to the environment.

### Scenario 7

You are a technical auditor in charge of penetration testing. You are contacted by a Product Leader who wants a penetration test to be carried out as quickly as possible because the product needs to be launched quickly. He asks you if it is possible to start the next day. You want to respond favourably to his request, but you're worried that the urgency will affect the quality of the work to be done.

#### ❑ What should you do?

A penetration test must be carried out within the framework of an audit agreement, which strictly defines the rules of engagement, the technical scope, the authorised/prohibited actions and the methods for carrying out the audit. This agreement ensures that the audit does not harm Renault Group, individuals, legal entities or the environment. In the absence of this agreement, you must redirect the Product Leader to the teams in charge of technical audits.

#### ❑ How can this scenario be avoided?

The activities of scoping, carrying out and reporting technical audits are fully integrated into the general project management processes and must be carried out within the necessary preparation and completion timescales. This ensures that the cybersecurity teams have sufficient time to carry out the technical audits in complete safety.

# 03 Principles and expectations

## 3.2.1 PROTECTION OF PERSONAL DATA: GETTING INVOLVED

### Principle 1: Developing and maintaining your knowledge and getting support

Anyone who, through their duties, is involved in IT projects must ensure that they acquire and maintain their personal data protection skills through any training required in accordance with national and/or international regulations and internal rules.

#### Scenario 1

As a Product Leader in the IT department, you need to move your project forward quickly. You realise that you have not taken the time to check the type of data being managed. Although you've heard of the 'privacy' network which supports projects, you haven't yet contacted your correspondent. Your project has been launched but you have not checked that it complies with the regulations on personal data, which potentially exposes Renault Group to the risk of non-compliance and sanctions.

#### ❑ What should you do?

- Take the mandatory e-learning "Fundamentals of the RGPD" training module.
- Look up the name of your Privacy Network contact (your department's Privacy Ambassador) on the platform dedicated to the protection of personal data and contact him or her for support throughout your project.

#### ❑ How can this scenario be avoided?

Following the mandatory training courses is an important part of our compliance system, in this case with a European regulation, and everyone must pay attention to it. If in doubt, don't hesitate to contact your manager to review the situation.

You can also sign up for the in-depth data protection training provided by the Privacy network.

# 03 Principles and expectations

## 3.2.2 PROTECTION OF PERSONAL DATA: RELYING ON THE ORGANISATION AND/OR GOVERNANCE

All employees responsible for a project must be familiar with their department's Privacy Ambassador. They should use the "Privacy by Design" checklist when developing software containing personal data, and should be familiar with and apply the "8 operational Privacy reflexes for a project manager". For example, they undertake to use only the data necessary for the project, to define a retention period and to apply protection measures that may be specific to the country in which they will be used. Close collaboration with the Privacy Ambassador is necessary to ensure that these rules are properly understood and applied.

**Principle 2: Using only data that is relevant to the service provided and for a defined period of time.**

### Scenario 2

You are project manager for a new connected service. The business needs to collect a lot of data for this service and you accede to their request without sufficiently investigating and "challenging" the business's needs.

Your Privacy Ambassador contacts you again a few days later and tells you that some of the data you are going to collect is not relevant to the operation of your connected service. The principle of data minimisation has not been fully applied. What's more, you haven't defined how long the data that will be used will be kept.

This is a potential non-compliance with the General Data Protection Regulation (GDPR), which impacts the privacy of the customers concerned, with the risk of penalties for Renault Group.

#### What should you do?

- Consult the documents available on the [DataPrivacy@Renault](mailto>DataPrivacy@Renault) platform. Check the data minimization and retention rules.

- You draw up a list of data that is strictly necessary for the project and ask for the others to be deleted.

#### How can this scenario be avoided?

- Know the applicable rules, so that you are attentive to the principles of minimisation and retention that protect personal data.
- Have each project using personal data validated by your department's Privacy Ambassador before it goes live.

# 03 Principles and expectations

## 3.2.2 PROTECTING PERSONAL DATA: RELYING ON ORGANISATION AND/OR GOVERNANCE

### Principle 3: Securing data and checking the countries in which it will be used

#### Scenario 3

You are a project manager developing a new application to optimise the charging time of new hybrid vehicles. You are working with a service provider in India who is in charge of carrying out tests. You transfer production data from existing customers to them, but without encrypting your file. You do not take into account the fact that the tests will be carried out in India and you do not consult your department's Privacy Ambassador.

The principle of personal data security has not been verified. This is a potential non-compliance with the GDPR, which has an impact on the privacy of the customers concerned, with the risk of penalties for Renault Group.

#### ❑ What should you do?

- Consult the documents available on the DataPrivacy@Renault platform, check the data security rules and define the procedure to follow if the data is processed in a country other than the one in which it was collected.
- You should immediately follow the training courses offered by the cybersecurity training school.

#### ❑ How can this scenario be avoided?

- Knowing the applicable rules, to be vigilant about the security and transfer rules that protect personal data.
- Each project using personal data must be validated by the Privacy Ambassador of the department and the RMSSI (Information Security and Safety Business Line Manager) before it goes into production.

# 03 Principles and expectations

## 3.2.3 PROTECTION OF PERSONAL DATA: ACTING RESPONSIBLY

All employees responsible for an IT project must inform the people affected by the project and provide the means for them to exercise their privacy rights.

### Principle 4: Keeping people informed

#### Scenario 4

You are developing a new "Vehicle To Grid" service for a recharging point. You have worked on publishing information about the functionalities of this new service for the customer: you have published this information on the application offering the service, but you have forgotten to publish it on the service's website.

The principle of informing people has not been fully applied. This is a potential non-compliance with the GDPR, which impacts the privacy of the customers concerned, with a risk of penalties for Renault Group.

#### ❑ What should you do?

- You must list all the websites and applications on which customers will be able to subscribe to the service or obtain after-sales service so as to include the necessary legal information.

#### ❑ How can this scenario be avoided?

- It is essential to be familiar with the sites and applications where the information intended for customers will be deployed.
- You should check with your department's Privacy Ambassador to ensure that this information is correctly deployed.

### Principle 5: Enabling the exercise of privacy rights

#### Scenario 5

You are the Product Leader of a connected service. You are working on a new version of this application.

You start your project without providing for the possibility of customers accessing their personal data via the application.

The principle of implementing the exercise of rights has not been respected. This is a potential non-compliance with the GDPR, which has an impact on the privacy of the application's users, with the risk of penalties for Renault Group.

#### ❑ What should you do?

- With your Privacy Ambassador, you organise a process that complies with the principles of the GDPR, enabling the employees concerned to exercise their rights over their personal data.

#### ❑ How can this scenario be avoided?

- Knowing the applicable rules well enough to create a process for exercising rights as soon as personal data is collected.
- Contacting your Privacy Ambassador for advice.

# 03 Principles and expectations

## 3.3.1 ARTIFICIAL INTELLIGENCE: GETTING INVOLVED

### Principle 1: Understanding, mastering and promoting AI within the Renault Group

AI is increasingly present in our lives, so Renault Group wants its IT staff to master what AI is, distinguish between the different types of AI and know how to promote it to the Group's employees.

To achieve this, Renault Group has set up a **progressive learning path for training, further training and professional retraining**.

As IT employees, we must not only train ourselves, but also share this learning path with our business contacts.

This pathway also highlights the limits of AI, i.e. the **challenges and opportunities** associated with this technology, as well as the **regulatory framework for AI in Europe**.

#### Scenario 1

You are a Product Leader and have been working with a business unit for a few months. Your business correspondents are aware of the value of their data and are convinced that AI can optimise some of their activities. They are aware of Renault Group's desire to accelerate the use of AI. However, they are wondering what they can do within their scope and how to go about it.

#### □ What should you do?

- You can recommend that they follow the **Artificial Intelligence training and awareness course**, the first step in acculturation. Then you can suggest that they go further with the AI Masterclass course on the fundamental concepts, challenges and opportunities of AI.
- You can then encourage them to contact the AI expert leader in order to become part of the Renault Group's **AI community** and benefit from all the Group's AI events.

#### □ How can you go further?

Your business correspondents can, if they wish, contribute to the training of other people in AI by becoming CaptAI or GenAI and thus position themselves at the heart of the deployment of AI in the Group.

# 03 Principles and expectations

## 3.3.2 ARTIFICIAL INTELLIGENCE: RELYING ON ORGANISATION AND/OR GOVERNANCE

### Principle 2: Integrating AI into the governance of digital projects

If not designed, deployed or used correctly, AI can lead to serious harm such as lack of transparency, discrimination, manipulation, privacy issues or environmental degradation. This is why Renault Group places great importance on building and using responsible AI.

Responsible AI governance has therefore been introduced. It is based on five major pillars: legal aspects, social equity, environmental impact, transparency and accountability, and model safety and robustness.

To put in place the best practices defined for designing, developing and deploying AI systems in a responsible manner, contact the community of AI referents.

### Scenario 2

You are a Domain Manager in an IT Division entity. You supervise a variety of business projects where project managers are looking to use AI to improve productivity or create new value-added business opportunities. In particular, you want to ensure that these projects comply with existing regulations and have a reasonable environmental impact.

#### ❑ What should you do?

- You can consult the **Responsible AI Playbook** and invite the project managers you work with to do the same.
- You can then use **the processes and tools recommended** within the Renault Group and referenced in this guide to ensure that your projects are Responsible AI from the outset.

# 03 Principles and expectations

## 3.3.3 ARTIFICIAL INTELLIGENCE: ACTING RESPONSIBLY

**Principle 3: Being aware of the risks associated with the use of AI in order to avoid any harmful impact on the company and its stakeholders.**

The AI Act is a European regulation on artificial intelligence adopted in 2024 to regulate the use of AI systems according to their level of risk:

- Unacceptably risky systems, such as social scoring, are banned.
- High-risk systems, used in critical areas such as health and safety, must comply with strict transparency, security and governance requirements.
- Limited-risk systems must inform users that they are interacting with AI.
- Minimal-risk systems are not regulated.

The regulation provides for substantial penalties for companies that fail to comply with the rules (fines of up to 7% of global turnover). It also includes the possibility for the authorities to withdraw products or services that do not comply with the requirements of the legislation.

In short, the AI Act is an ambitious regulation for the use of AI systems, aimed at protecting citizens while enabling innovation and competitiveness in Europe.

The best practices and recommendations relating to the use of AI are referenced in the **Practical Guide to Responsible AI (or Playbook)**. Please refer to it and contact the people in charge of responsible AI.

### Scenario 3

You are a Product Leader working on the development of an AI system for handling complaints in the after-sales service department. It seems that the system gives less attention to complaints from female customers about mechanical problems and the same attention to complaints from male customers about electronic problems. You suspect a gender bias in the way complaints are handled. Yet you know that this new AI is eagerly awaited by the business and you want to meet the approaching production launch date.

#### ❑ What should you do?

- The AI Act emphasises that the training and validation data for the AI model must be relevant, representative and of high quality in order to mitigate any risk of bias. Despite the pressure of deadlines, you should therefore refrain from going into production for the time being and check the robustness of your model.
- You should get in touch with the data scientist in charge of the model to check your suspicions. Weighting the data could allow you to adjust the dataset and avoid these biases.

#### How can this scenario be avoided?

- It is the Product Leader's responsibility to ensure that all the steps involved in creating the AI system, i.e. training, validation and testing, have been followed and that the Data Scientist has checked the quality of the data to avoid any risk of bias.
- The Product Leader can draw on the Golden Rules set out in the Playbook, which clearly specify the responsibilities of each player and indicate that AI systems must be "fair and inclusive".

# 03 Principles and expectations

## 3.3.3 ARTIFICIAL INTELLIGENCE: ACTING RESPONSIBLY

### Scenario 4

You are a developer in the team in charge of an application for salespeople in dealerships. This application must provide them with a turnkey sales pitch, adapted to the customer's profile. The sales staff have received the new AI. They tried to use it on a few intuitive cases but didn't understand how it worked. They're not convinced of its relevance, so they don't use it with their customers.

#### ❑ What should you do?

- You need to ask the Product Owner, with the support of the Data Scientist, to draw up instructions for using the AI system. You can leave the system in production, but you must correct it as quickly as possible in order to bring value to your users.
- Under the AI Act, the designer of an AI system has a duty of transparency and information on the interpretation and use of the system. The system must be designed in such a way as to be understandable to end-users and enable effective human supervision, which means making it easier to interpret and explain.
- In our case, the Data Scientist will be able to indicate in the documentation which criteria are influential in the AI model and how to associate the model's output results with customer arguments.

#### ❑ How can this scenario be avoided?

- The Product Owner and the Product Leader should have written the user documentation to enable the AI system to be used with peace of mind.
- The Product Leader can rely on all the Golden Rules formalised in the Playbook, which specify the duty of "transparency and responsibility" for AI systems. The aim is to enable the user to understand and explain the decisions made by the AI system, using clear examples that are accessible to everyone.

# 03 Principles and expectations

## 3.4.1 RESPONSIBLE DIGITAL : GETTING INVOLVED

### Principle 1: Being aware of the impact of digital technology to improve your practices

Renault Group is offering its employees a **training and awareness-raising programme on the environmental and social challenges of digital technology**. This course is aimed primarily at IT staff, as they are responsible for the responsible design of digital services.

A community of Responsible Digital Advisors has also been set up within the IT Department to roll out the Responsible Digital approach and build a common culture.

These training courses and this community should be used as a basis for questioning or discussing the environmental and social impacts of designing, purchasing or operating a digital solution.

### Scenario 1

You have recently started work on a new project. You are sensitive to the issues of global warming and last year you took part in a climate mural. You know that your application must meet the needs of users by complying with Responsible Digital Criteria, and you're wondering how to get started.

#### ❑ What should you do?

- You should follow the Digital Responsibility awareness and training courses and, for example, sign up for a "Digital Mural" workshop.
- You should contact the community of Responsible Digital Coordinators and receive support in promoting the use of best practices among your colleagues, identifying areas for improvement to reduce data consumption or storage and proposing more energy-efficient architectures or algorithms.

#### ❑ How can you go further?

You can also sign up for a certification course from the Institut du Numérique Responsable.

# 03 Principles and expectations

## 3.4.2 RESPONSIBLE DIGITAL: USING THE ORGANISATION AND/OR GOVERNANCE

### Principle 2: Integrating digital responsibility into the governance of digital projects

A successful Responsible Digital approach means integrating the notion of sustainability into the Renault Group's decision-making processes. This means that we have to **take sustainability criteria into account when evaluating our digital solutions** in order to meet a threefold challenge: controlling the impact and ensuring the long-term viability of our business, while accelerating the Group's digital transformation.

Taking this into account means systematically measuring the environmental and social impact of our digital solutions, and to do this we need **reliable measurements**.

In addition to actions to reduce our own environmental and social footprint (Sustainable IT), our digital activities must **contribute to reducing the footprint of the Group's other activities** (IT for Sustainability).

By providing innovative digital solutions, we can support the business functions in their transformation and impact reduction objectives set out in the Renault Group Climate Plan.

### Scenario 2

You are a Domain Manager in an entity of the IT Department. On a day-to-day basis, you steer and manage the development of part of the digital portfolio, as well as the associated budget. You want to take sustainability criteria into account when evaluating digital solutions, and you want to know how to go about it in practical terms...

#### ❑ What should you do?

- You need to draw on the expertise of the digital teams and the environmental indicators available to factor sustainability criteria into your decisions. You need to identify the risks and ask them to take the necessary steps to remedy them: reducing the solution's carbon footprint, complying with accessibility practices, etc.
- Your team should use the measurement tools made available within the Group: calculator of the environmental impact of an initiative or project (BUILD phase), monitoring of the carbon impact of resources deployed in the Cloud (RUN phase), Digital Responsibility Maturity Score for the product team, etc.

❑ **How can we go further?** As innovation is a value supported by Renault Group, you can, as Head of Domain, encourage the business to undertake decarbonisation projects (IT for green).

# 03 Principles and expectations

## 3.4.3 RESPONSIBLE DIGITAL: ACTING RESPONSIBLY

### Principle 3: Adopting the "Sustainable by Design" approach

1. Renault Group is committed to a more responsible approach to IT. This new approach is reflected in **the eco-design approach**, which aims to create digital services that are more respectful of the environment, less costly and offer a better user experience.

Every employee who contributes to the design, development or operation of a digital solution must strive to integrate these principles throughout the solution's lifecycle, from conception to end-of-life.

To this end, a set of best eco-design practices is shared throughout the Group on the **Responsible Digital @ Renault** platform. This set should be used to guide the actions to be taken in terms of conception, architecture, design, development, Cloud hosting, etc. For some projects, this can reduce the solution's carbon footprint and Cloud operating costs by more than 70%.

2. **The transparency of our Responsible Digital Practices** is an important competitive advantage in attracting new customers and new employees. It also enables us to meet the expectations of our employees and to combat '*greenwashing*'.

The digital solutions we deliver must encourage our customers to adhere to our Responsible Digital approach by clearly communicating our commitments and offering features that enable them to play an active role in this approach (use of eco modes, dark mode, deactivation of superfluous notifications, etc.).

3. Everyone should **integrate sustainable practices into the use of** the IT equipment and tools made available to them.

Guides and guidelines are available for this purpose: use the camera wisely in meetings, reduce the power consumption of your equipment, take care of your equipment to extend its lifespan, take part in Digital Clean-up Day to learn how to clean up your data.

# 03 Principles and expectations

## Scenario 3

As a Software Architect, you join the development team for an existing product. You consider that this product is potentially very resource-intensive (computing, storage, etc.) and may involve significant infrastructure costs and carbon footprint. You note that no means of measuring the performance of the code has been put in place, and that good practice does not seem to be well known. You also note that the implementation of probes has been omitted from the list of features. This would make it possible to measure, in production, the real consumption of the code and to size it as accurately as possible.

### ❑ What should you do?

- Consult the eco-design guidelines available on the Responsible Digital @ Renault platform to find the recommendations concerning the software architecture.
- Suggest "Eco" options such as "Dark Mode" or notification frequency settings to reduce power consumption and network traffic.
- You will contact the Product Leader and Product Owner to propose these changes, which will help to involve users and contribute to the dissemination of our values and know-how. You will also propose the introduction of "Eco" functions and encourage users to adopt "Eco" modes. This is an opportunity to spread our values and know-how.

### ❑ How can this scenario be avoided?

- By encouraging the team to follow training courses in eco-design of software, or training courses of the "Software Craftmanship" type to develop in-house skills.
- By reminding them of the importance of integrating best practice at the earliest stages of the project (particularly at the design stage).
- In addition to the probes mentioned above, by requesting the implementation and monitoring of KPIs relating to the performance and footprint of the code (essential for reducing its impact).
- Finally, by contacting the digital referent responsible for your scope to implement these various points.

# 04 Reference Documents and whistleblowing alert system



# 04 Reference Documents and whistleblowing

## CYBERSECURITY

### Training courses

- Cyber and me

### Standard

- Renault Group Cybersecurity Policy (see « Cybersecurity » sharepoint)

### Contacts

- Report a cybersecurity incident by email to [incident.cyber-security@renault.com](mailto:incident.cyber-security@renault.com)

## ARTIFICIAL INTELLIGENCE

### Training courses (Learning@RG)

- **AI acculturation:** « AI for all at RG »
- **AI in depth:** AI Masterclass & Reknow University Certificate
- **Generative AI practice:** Workshop GenAI for ALL
- **Day2Day experience:** E-learning modules (linkedin)

### Standard

- [AI community](#) Sharepoint

### Contacts

- [ai-community@renault.com](mailto:ai-community@renault.com)

## PROTECTION OF PERSONAL DATA

### Training course (Learning@RG)

- Fundamentals of the GDPR

### Standards

- [Personal data protection policy](#)
- [DataPrivacy@Renault platform](#)

### Contacts

- [Privacy Ambassadors](#)

## DIGITAL RESPONSIBILITY

### Raising awareness and training

- [Digital Collage Workshop](#)
- Digital Responsibility Training Pathway : [FR](#) or [EN](#)

### Standards

- [Digital Responsibility Framework](#)

### Contacts

- [referents@grouperenault.onmicrosoft.com](mailto:referents@grouperenault.onmicrosoft.com)
- [Find your Responsible Digital Coordinator](#)

# 04 Reference Documents and whistleblowing alert system

## THE WHISTLEBLOWING ALERT SYSTEM

Any person listed below may make a confidential report under the Renault Group whistleblowing system.

This system is accessible to all employees, former employees, unsuccessful candidates for 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 seconded employees, etc.), co-contractors (e.g. dealers or suppliers/service providers) and their sub-contractors. It complements the channels for reporting misconduct, which are management, human resources, employee representatives, the Ethics and Compliance Department and the Professional Alert Department.

## Conditions for acquiring whistleblower status

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

1. You must be a physical person. Report or disclose facts that have occurred or are very likely to occur, 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. have obtained the information in the course of his or her professional activity. Where 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 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 *renaultgroup.com website / Commitments / Ethics section* or by flashing the QR Code:



## Protection of the whistleblowers

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 alert. Whistleblowers are treated in strict confidence, subject to applicable legal obligations and any legal proceedings. Whistleblowers also benefit, where applicable, from civil and criminal immunity as well as protection against the risks of reprisals and discrimination.

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

# 04 Reference Documents and whistleblowing alert system

## PERSON RESPONSIBLE FOR THE CODE WITHIN RENAULT GROUP

The Renault Group Senior Vice President, Information Systems and Digital Operations is the "owner" of this Code of Conduct for IT and Digital. He is responsible for amending and updating it.

If you have any questions or require information relating to the Code of Conduct for IT and Digital, please contact him/her.

