GROUP CODE OF CONDUCT

Version n°2

SODIAAL

Coopérative Laitière Française

2021

CONTENTS

HOW SHOULD THIS BE USED ?

HOW SHOULD THIS BE USED?

THE CODE OF CONDUCT IS A REFERENCE TOOL THAT ALLOWS EACH OF US TO ACT WITH INTEGRITY BY QUESTIONING SITUATIONS ENCOUNTERED IN OUR ACTIVITY

Some situations are difficult to handle. Making ethical decisions sometimes seems difficult, as it involves more than just following a set of rules.
The Code of Conduct is a reference tool that allows each of us to act with integrity by questioning situations encountered in our activity. In addition to the Code of Conduct, Sodiaal has put in place a set of policies and procedures that we must follow. Finally, in order to make the right decision, you should not hesitate to ask questions whenever necessary, so that you act in the right way, at the right time and for the right reasons.
In some situations, the guidance provided in this Code of Conduct may differ from local laws or customs in a country. If local law or custom imposes more restrictive standards than those set out in the Code, local law or custom shall prevail. If, on the other hand, the Code provides for a more restrictive provision, the latter will prevail.

IF IN DOUBT, ASK YOURSELF THE FOLLOWING QUESTIONS:

- Am I in violation of any law, Sodiaal's Code of Conduct, policies and procedures?
- Am I consistent with the ethical values?
- Do I behave with others as I would like to be behaved with?
- Do I owe anything to anyone?
- Would my decision seem inappropriate if it were published on the front page of a newspaper?

IF THE ANSWER TO ANY OF THESE QUESTIONS RAISES CONCERNS, DON'T KEEP IT TO YOURSELF, **TALK ABOUT IT**.

HOW DO WE ALERT? (see "Ethics Alert").
> Alert telephone number: 0800 94 16 50
> Alert e-mail address: conformite@groupesodiaal.fr

It is up to each of us to know and understand its content. If we believe that one or more of our ethical principles are not being respected, we have a duty to report this.

This Code of Conduct defines the guiding principles for the development and construction of the Sodiaal Group: It applies to every employee, who must therefore act with discernment in all critical situations that he or she may encounter in his or her relations both inside and outside the company.
The Code of Conduct is integrated into the Group's Internal Regulations.
It was validated at the Comex meeting on 2 November 2021.
If in doubt about the application or interpretation of a rule, consult the Internal Control and Compliance Department before acting.

I.

THE ESSENTIALS OF SODIAAL GROUP

Sodiaal is a cooperative that brings together 20,000 dairy farmers and 10,000 employees. Our cooperative model is based on strong human values, where people are central to the organisation, and also on ethical values that unite us around a common objective: to be "People to better feed people":

- solidarity and equity
- respect
- trust
- transparency
- boldness

These values, shared by all, must guide our daily actions in the accomplishment of our mission: " *to enhance the value of the milk of all members in order to guarantee them an income that best remunerates their work, and to increase and share the profitability of the company in a sustainable manner* ".
In order to reaffirm this commitment to its values to its employees, customers, suppliers and other stakeholders, the Sodiaal Group has drawn up this Code of Conduct, which sets out the best practices to be followed individually and collectively in order to contribute fully to the success of our cooperative model and our corporate project.

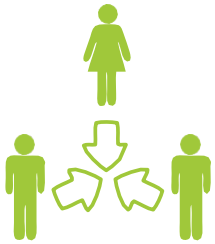
The Code of Conduct expresses the Sodiaal Group's responsibility towards all the stakeholders in its business, which are:

1.Employees

The Sodiaal Group intends to promote and maintain a stimulating, creative and non-discriminatory working environment for all employees and partners, respecting diversity and the dignity of the individual.
At all levels, the Sodiaal Group is committed to maintaining human relations that are both demanding and respectful. In this context, it is everyone's responsibility to ensure that all employees are able to carry out their work in good physical and moral conditions. In exercising responsibilities and hierarchical relationships, the individual must always be respected.

2.Consumers and customers

The Sodiaal group ensures the food safety and quality of its products, respecting legal and regulatory provisions and internal procedures. Our products must be consumed without risk to health.



3.Suppliers, service providers and partners

The Sodiaal Group makes the exercise of its commercial relations conditional on compliance with local legislation, internal charters and international standards in the field of human rights and working conditions, the environment and ethics.

The Sodiaal Group is committed to building a fair and sustainable relationship with its suppliers based on the Responsible Supplier Relationship Charter, developed by *Médiation des Entreprises* (Business Mediation) and signed by the Group.

The Sodiaal Group also asks suppliers and partners to commit to respecting the Sodiaal Group's Code of Conduct, to act against corruption in all its forms, against the employment of minors and forced labour, and to respect the new General Data Protection Regulation (GDPR).

4.Civil servants and state representatives

The Sodiaal Group is committed to establishing exchanges based on honesty and integrity and ensures strict compliance with laws and regulations.
These commitments must be reflected in the involvement and ethical behaviour of each Group employee in all circumstances.

5. Adopt responsible conduct with regard to the regions in which it operates

In its international development, the Sodiaal Group is committed to adopting a responsible attitude towards the countries in which it operates.
The Sodiaal Group ensures that its subsidiaries comply with the laws and regulations applicable in each of the countries in which it operates.

The Sodiaal group participates through its activities in the economic and social development of the communities where its facilities are located, with a view to long-term development.
The Sodiaal group refrains from making any commitment or support of any kind whatsoever in favour of a party, political or religious group.

II

WORK IN COMPANIES

The Sodiaal Group promotes relations between colleagues based on courtesy, consideration, recognition and discretion. The Sodiaal Group condemns harassment of any kind.
Respectful of diversity and privacy, the Sodiaal group considers above all the competence of its employees and refrains from any form of discrimination.
The Sodiaal group is also committed to diversity within its organisation and considers the differences between its employees as an essential asset for the success of a responsible company.
In addition, the Sodiaal group promotes diversity and equal opportunities for each employee or candidate in terms of recruitment, access to training, remuneration, social protection, internal mobility and career development.

1.Personal responsibility

Each employee must carry out his or her duties with honesty, care, diligence, professionalism, impartiality and ethics.

2. Compliance with laws and regulations

Each employee of the Sodiaal Group must be familiar with the laws, regulations and obligations related to his or her task. Any activity that could lead the Group into an illegal practice is strictly prohibited.

3.Customer relations

The Sodiaal Group is committed to treating all its customers honestly and fairly, regardless of the size of the company. It is committed to providing its customers with quality products and services that meet their requirements. Confidential, sensitive or private information relating to customers must never be communicated to others by an employee of the Sodiaal Group, except when required by a competent authority or authorised in the context of a project or contract.

4.Supplier relationship

Human relations are considered a major asset for the Sodiaal group, which wants its exchanges with its suppliers to rhyme with commitment and shared values.
The Sodiaal Group's expectations of its suppliers are primarily focused on the quality of their services and products.

The supplier undertakes to respect and ensure respect for the commitments of the Sodiaal Group by all of its employees, as well as by any person or entity involved in the execution of the contracts concluded between it and our Group.

III

HEALTH AND SAFETY

Health and Safety is one of the Group's priorities in the implementation of its "Safety First" policy. Thus, the Sodiaal group is committed to guaranteeing a safe and healthy working environment at all its sites, with an equivalent level of requirements for each site. The Sodiaal Group is making the necessary efforts to ensure the protection of employees, to develop good practices and to correct risky conditions wherever they work.

In order to ensure that appropriate safety behaviour is put into practice, the Sodiaal Group implements "Behavioural Safety Visits". It is a management tool and a time for exchange between employees and managers to study methods, organisations and the work environment in a real situation. Trained staff are committed to carrying out these visits.

Each employee has an obligation to report hazardous situations that he or she witnesses or incidents that reveal such situations, and to contribute to the implementation of preventive actions. Compliance with safety instructions is a strict obligation.

This commitment also applies to temporary workers, external companies and visitors.

IV

ENVIRONMENT AND SOCIETAL RESPONSIBILITY

1.Environment

Respect for the environment is a priority for the Sodiaal group.
The Sodiaal group is committed to respecting the regulations and standards in force with regard to the environment, particularly in terms of:

- energy, water and chemical consumption,
- air emissions, liquid discharges, noise and odour pollution and soil pollution
- waste treatment
- preservation of biodiversity, etc.

It is constantly seeking to improve the environmental management of its operations, including reducing its carbon footprint throughout the chain and designing and marketing recyclable packaging.

2.Societal responsibility

The Sodiaal group is committed to a continuous improvement process, which aims to improve knowledge and reduce the environmental and social impacts of its activities. This approach is structured around 3 themes, with the aim of covering all the priority issues identified for the Group (see below).

As regards the upstream perimeter of the sector and the production of milk on the farms of our member farmers, the Sodiaal group has implemented a voluntary approach called "La Route Du Lait" (“The Milk Route”) since 1998. All of Sodiaal's member farmers are involved and are thus committed to product quality, respecting sustainable development, and taking into account health guarantees, hygiene, animal welfare, respect for the environment and good farming practices.

FUTURE-FOCUSED FARMS

Good for people
Value creation & sharing, sustainable collection, young farmers

Preserving the planet
Low carbon, high-biodiversity, resilient & self-sufficient livestock

Respect for animals
Exemplary animal welfare, alternatives to antibiotics

PRODUCTS FOR THE BEST OF MILK

Bringing the best to our consumers
Quality, nutrition, naturalness

Low environmental footprint
Carbon footprint, water, packaging, fight against food waste

Responsible purchasing
Supplier evaluation, responsible supply chains, charter & ethics

PROUD & COMMITTED COMMUNITY

Quality of life at work
Health and safety, non-discrimination, well-being at work

Community spirit
Pride of ownership, opening up of capital

Career paths & expertise
Professional mobility, training, internal transmission

Each employee is encouraged to take note of the Sodiaal Group's commitments in terms of social and environmental responsibility and to do their utmost to contribute to respecting them in the context of their activity.
In addition, our suppliers undertake to respect and ensure respect for these commitments within their own area of responsibility, in accordance with the provisions in force in the areas where they operate.

The *Déclaration de Performance Extra-Financière* (DPEF - Extra-Financial Performance Declaration), audited by an independent third party and published annually, reports on the Sodiaal Group's commitments, their possible updating, as well as the main actions and achievements of the past year in terms of social and environmental responsibility.

3.No waste

All employees are encouraged and sensitised to make appropriate use of the resources at their disposal, while respecting the needs of their activity.

In the context of the so-called "duty of care" law (2017), the Sodiaal Group publishes its annual duty of care plan in order to identify and prevent the risks of serious harm to the environment, fundamental freedoms, and the health and safety of people that may result from the activities of the Group, its subsidiaries and its suppliers and service providers.
Information on Business Ethics, Corporate Social Responsibility, Occupational Health and Safety and our alert mechanism can be found in the duty of care plan.

V

BUSINESS INTEGRITY

1.Anti corruption

Sodiaal Group and its suppliers undertakes to comply with the obligations stipulated by law No. 2016 1691, known as the Sapin 2 law, published in the Official Journal on 10 December 2016 and has implemented different means to prevent and fight corrupt practice.

Corruption involves:

- The granting of any advantage (money, promise, donations, gifts, debt removal, under-invoicing, invitations, etc.)
- To a private or public person who can influence a decision
- To perform or not perform an act connected to their activity or their position

Corruption is prohibited, whether active (corrupting) or passive (corrupted).
All corruption practices, including attempts, are forbidden and heavily punished by law (imprisonment, fine, forfeiture of civil rights, notably).
The consequences of such practices on Sodiaal Group, particularly in terms of commercial reputation and image, would be extremely damaging.

2.Donations, sponsorship and political contributions

As a responsible corporate citizen, the Sodiaal Group is committed to supporting the development of people and communities, but is committed to ensuring that its donation and sponsorship activities are carried out in strict compliance with applicable anti-corruption laws.

In order to guarantee the impartiality of political life, the Sodiaal group does not pay any funds or provide any services to political parties, holders of a public mandate or candidates for such a mandate, even if the legal nature of such contributions is recognised under the laws of the country where such payments are likely to be made.

.

SOME EXAMPLES OF RISK SITUATIONS:

✗ Application for funding from a sports club or association or in exchange for a promise of preferential treatment in a public or private contract.
✗ Promise of employment or internship contract in return for purchase of product or acceptance of a higher price.
✗ Gifts, invitations in the hope of signing a contract or obtaining a permit.

3.Influence peddling

An offence very similar to bribery, but involving the use of a public official as an intermediary.
Influence peddling: a third person, a public official, intervenes with a public authority or administration to obtain a decision. The intermediary presents himself as a person with influence to obtain a real or supposed favour.
More specifically, it is recalled that the Sodiaal Group has already put in place the following rules which must be respected by all Group employees:

RELATIONSHIP WITH A MANDATE HOLDER OR PUBLIC AUTHORITY AND/OR ITS REPRESENTATIVES

Any Group employee who enters into communication with persons in administrative or governmental positions in the context of interest representation activities must comply with the regulations applicable in the countries in which they operate. In particular, any practice of representing interests on behalf of the Group must be duly documented and the documentation sent to the Internal Control and Compliance Department for retention.

Rules to be applied:

- Any relationship that is of a nature to obtain a particular advantage is prohibited.
- Any professional relationship exceeding the threshold of 10 meetings per year with the same interest representative should be prohibited.
- Relationships related to the security of goods and persons are allowed and are not part of this monitoring.

FIGHT AGAINST ILLICIT PAYMENTS

The Sodiaal Group's policy is to ban all forms of illegal payments and practices (in France and abroad). The companies and employees of the Group must not offer an advantage or respond to the solicitation of any person who, claiming to have real or supposed influence with a public or private person, proposes to use his or her direct or indirect influence in order to obtain contracts or any other decision.

4.Gifts and invitations

Gifts, invitations and meals cannot be accepted or offered if they exceed the set amount of 60 euros per person per year.
Where for compelling reasons it is difficult to comply with the limit, it is imperative to be fully transparent and to declare all gifts, receipts or invitations received (valued in good faith) or given in excess of the Group's limit to the line manager and record them in an ad hoc register. The register must be completed in such a way that it can be read by a third party to the company and specifically by a supervisory body.

Rules to be applied only to gifts and invitations outside the Sodiaal group:

A gift offered or received may not exceed the maximum threshold set, unless the prior agreement of the line manager has been duly given (in writing or by e-mail, to be kept by each department manager). This applies to all types of gifts, for example:

- Invitation to a meal; if there is any doubt about the value of an invitation received, it is preferable to ask for the prior agreement of the line manager as a precaution
- Invitation to a sporting or cultural event
- Invitation to a commercial or public relations event, etc.
- Gift vouchers
- End of year gift
- Any invitation with a spouse
- Any invitation with a value of more than €60
- Any repetition beyond 4 invitations from the same person
- etc.

A gift or invitation received in excess of the set limit (60 euros per year and per person) should be refused spontaneously if possible. If it is accepted, it must be recorded even if it is distributed or shared with other employees. The words "has been distributed or shared" must be entered in the register, as well as the service or recipients concerned.
All gifts given or received must be recorded in the register if they exceed the limit.

The following practices are not allowed:

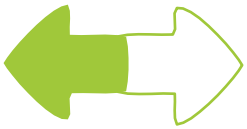
- Giving a gift or entertainment to an official agent to facilitate certain procedures.
- Offering a gift or entertainment to influence a business/government decision.
- Inviting one of the family members of an existing or potential customer/supplier to attend a cultural or sporting event, etc.
- Accepting an invitation before or during a tender on which it is possible to have an action/influence.
- Personally paying for a gift or entertainment in order to avoid having to comply with the Code of Conduct.
- Obtaining discounts on products or services that are not available to all employees.
- Obtaining gifts or entertainment of an inappropriate nature or in inappropriate locations.

TYPES OF PRACTICES AND BEHAVIOURS THAT ARE PROHIBITED

✗ Illicit advantages and payments: it is forbidden to offer or propose advantages or to respond to the solicitation of any person who would propose to use his or her real or supposed influence with a private or public person to obtain any decision such as signing a contract, authorisation, non-participation in a call for tenders, etc.
✗ The provision of services free of charge or at a much lower price than the market price
✗ Small but recurring benefits (invitations)
✗ Gifts in kind (watches, trips, company shares, etc.)
✗ Payment of debts

GOOD PRACTICE AND PERMITTED BEHAVIOUR

✔ Respect for the brand image and good reputation of the Sodiaal group
✔ Compliance with the rules of ethics set up by the Sodiaal group, of loyalty and transparency
✔ Clear rejection of any suggestion of active and passive corruption or fraud or conflict of interest
✔ Use, if necessary, of the alert system made available to the employees of the Sodiaal Group. (See page 34)
✔ Compliance with applicable laws and regulations in the countries of operation
✔ Respect for cultures and environments in the countries of operation



5.Conflicts of interest

A conflict of interest is a situation in which the interests of the Sodiaal Group diverge from the personal interests of our employees or their relatives. Our staff must not be put in situations that prevent them from remaining objective and impartial in the performance of their duties.

They should alert their superiors to any potential conflict of interest situation and should not interfere in the decision-making process.

6.Competition law

The Sodiaal group respects the legal and regulatory provisions, both national and international, relating to competition law in order to have fair and equitable exchanges within the framework of free competition.

The objective of competition law is to protect the functioning of healthy and fair competition between companies.

Competition law severely punishes behaviour by companies or employees of companies that distorts fair competition to the detriment of customers, suppliers and finally consumers.

In the event of infringement of the competition rules, the French Competition Authority and the European Commission can impose very high fines and injunctions to cease and desist. The ordinary courts may order the offending company to pay damages and impose criminal penalties on individuals if they intentionally played a personal and decisive role in the design, organisation and implementation of the anti-competitive practices (up to a fine of €75,000 and four years' imprisonment).

The Sodiaal Group has made two fundamental commitments: to behave in a free and competitive manner and to implement a competition law compliance programme, the main elements of which are as follows:

- **Commitment of managers and raising awareness of staff**
- **Appointment of a Compliance Programme Manager**
- **Implementation of training modules on competition law rules, including annual training by e-learning,**
- **Adaptation of the internal rules to mention the sanctions incurred in case of participation in a violation of the competition rules**
- **Creation of an alert prevention system**
- **Insertion in employment contracts of specific provisions concerning compliance with competition rules, monitoring information and participation in the warning**
- **Involving our suppliers in our ethical approach**

ANTI-COMPETITIVE AGREEMENTS

Illegal agreements are any agreements, formal or informal, between independent undertakings which have as their object or effect the restriction of competition in a market.

There are two types of agreement:

- Horizontal agreements: these are written, verbal, tacit or informal agreements between competitors.
- Vertical agreements: these are written, verbal, tacit or informal agreements between independent companies located at different levels of the commercial chain (e.g. between a supplier and its distributor).

ABUSE OF A DOMINANT POSITION

Abuse of dominance is when a company uses its strong position in a market to foreclose it, to drive out competitors or to prevent new entrants.

Two conditions are necessary: the existence of a dominant position and the existence of an abuse.

There are several criteria for demonstrating dominance, the main ones being:

- The market shares of the company that engaged in the practices
- The difference between the market share of the undertaking in question and that of its competitors
- The brand image, the reputation of the company, etc.

Abuses include: refusal to sell or provide services without an objective reason, predatory, excessive or imposed prices, tied selling, loyalty discounts, exclusivity, discriminatory practices and denigration, etc.

PROHIBITED PRACTICES AND BEHAVIOURS

In relations with competing companies:

✗ Exchanges of sensitive information (purchase prices, sales prices, volume, margins, strategies, costs, monitoring of negotiations with distribution)

✗ Agreements, even if tacit, which involve the joint fixing of prices or trading conditions, the sharing of geographical markets or customers, the limitation of production, capacity, markets, investments or technical progress

✗ Discussion or consultation between competitors before the submission of tenders

✗ Participation in a boycott of a customer or supplier

✗ Agreement or discussion on an average purchase price for raw materials

In vertical relationships with reseller customers or suppliers:

✗ Imposing a minimum selling price or fixing the distributor's margin

✗ Pressuring/offering financial incentives to bring prices in line with recommended selling prices.

PERMITTED PRACTICES AND BEHAVIOURS

In relations with competing companies:

✓ The use of price or market trends and indices for individual pricing

✓ The collection and/or transmission within professional organisations of information on past (6 months or more) and aggregated prices and volumes or publicly available information (press etc.)

✓ The implementation of cheese volume control plans to better manage milk volumes in relation to the PDO volumes that the PDO sector can sell

✓ Conducting market research

In vertical relationships with reseller customers or suppliers:

✓ The transmission of recommended selling prices provided that it is not repeated

✓ The explanation of the pricing policy

✓ Negotiating discounts and rebates

PRACTICAL RECOMMENDATIONS:

During official meetings or informal exchanges with the various parties involved in the market:
Ensure that meetings are held with an agenda that does not include prohibited practices. Stick to the agenda. Minutes should be kept of each meeting.
If anti-competitive practices are implemented or even discussed during the meeting, immediately ask for the discussions to be stopped, expressly state your disagreement and ensure that it is recorded in the minutes of the meeting. Leave the meeting if necessary and have your departure recorded in the minutes of the meeting.

When concluding certain cooperation agreements:
For agreements on pooling of production resources, industrial cooperation agreements, joint purchasing agreements, joint R&D or marketing agreements and any agreement requiring exchanges of information between competitors, the legal department should be consulted.

In the event of an investigation by the competition authorities:
Competition investigations are similar to searches in which investigators visit offices, seize documents and may question those present. Competition investigations are often anxiety-provoking and it is important to remain calm.

7.Fraud

Fraud consists of deliberately deceiving others to obtain an illegitimate benefit, or to circumvent legal obligations or organisational rules. Fraudulent behaviour therefore requires a factual and intentional element as well as a process of concealment of the unauthorised act.
The Sodiaal Group does not tolerate fraudulent practices in the conduct of its business. It implements the necessary measures to reduce the risks and effects.

Combating fraud is an imperative. In addition to the financial risks involved, the risk of fraud could damage the integrity of the Group, its reputation and the trust placed in it by its customers, affiliates or any other party.
You can therefore see the commitments of the Sodiaal Group in the fight against fraud in the Anti-Fraud Charter.

EXAMPLES OF PROHIBITED SITUATIONS:

- ✗ When signing a contract with a client company, its representatives express the wish to transform a discount you have granted into a benefit in kind (e.g. free delivery of products).
- ✗ To increase the chances of completing a transaction with authorities, someone strongly suggests an association with a designated local partner.

8.Money laundering

Money laundering is the process of **concealing the nature and origin of money derived from illicit activities** (drug trafficking, arms trafficking, human trafficking, tax evasion, illegal labour, corruption, illegal speculation, etc.) by incorporating this "dirty money" into legal activities. The aim is to **give it a legal appearance and to conceal its origin and real owner** (via false invoices, shell companies, etc.).

The **financing of terrorism** is the provision of goods, services or funds that may be used for terrorist activities.

The **Group prohibits and strongly condemns** all practices of this nature.

Money laundering represents a risk for Sodiaal, which must in no way be accused of promoting the financing of prohibited activities, such as terrorism, drug trafficking or the financing of certain political parties.
This risk is criminal in nature, with **penalties of up to ten years' imprisonment and a fine of EUR 750,000** for individuals. The revelation of such an offence would also cause **significant damage to the interests and image of Sodiaal**.

GOOD PRACTICE AND PERMITTED BEHAVIOUR

- ✓ Being constantly vigilant
- ✓ Conducting integrity checks on our business relationships, prior to any engagement, to ensure that they are legitimate activities and that the money is not from illegal activities or sources subject to international sanctions. Obtaining and analysing supporting documents for our business relationships.
- ✓ Establishing a monitoring and alert system, particularly for atypical or suspicious transactions and transfers of funds from or to geographical areas considered risky.
- ✓ Consulting the MAF risk country lists.
- ✓ Report any suspicions or doubts to your line manager or to the Internal Control and Compliance Department.

TYPES OF PRACTICES AND BEHAVIOURS THAT ARE PROHIBITED

- ✗ Concealment of payments through the use of third parties.
- ✗ Accepting cash transactions, except in special cases and in full transparency with our hierarchy.
- ✗ Accepting unusual payments without prior analysis and verification of supporting documents.

SOME EXAMPLES OF AT-RISK SITUATIONS

- ➢ Transfers of funds from or to geographical areas considered risky.
- ➢ Operations or activities requiring cash payments.
- ➢ The use of "cashboxes".
- ➢ Transactions structured to circumvent reporting obligations.
- ➢ Unusually complex transactions or transactions involving unusually large amounts.
- ➢ Transfers to and from numbered accounts.

9.Confidentiality and use of official information

Confidentiality of information is a priority for the company.
Each employee is responsible for protecting sensitive and/or confidential information belonging to and/or relating to the Sodiaal Group and the companies that make it up, their activities, strategies, policies, products or other, regardless of the medium or nature of the information. Thus, all users of the Sodiaal Group's information and communication systems must behave in a professional and responsible manner, taking care to preserve the image of the Sodiaal Group, its activities, its products, its brands and its employees.

GOOD PRACTICE AND PERMITTED BEHAVIOUR

- ✓ Treat confidential matters with the utmost caution in external environments (e.g. on trains, planes, in restaurants, at conferences).
- ✓ Seek advice from the Legal Department on the need for a confidentiality agreement.
- ✓ Report to your line manager any situation that may indicate that the protection or confidentiality of sensitive information may have been affected.

10.Preventing conflicts of interest

Each employee must exercise his or her responsibilities in good faith and with loyalty to the Group and must ensure that he or she is protected against any conflict of interest.
A conflict of interest exists when, in the context of his or her professional activity, the employee's personal interests are directly or indirectly in contradiction or competition with the interests of the Group and may therefore influence the position or decision he or she is led to take or not to take and call into question his or her loyalty.

These personal interests may result from financial or professional commitments, family or sentimental ties, or political or ideological affiliations.

Conflict of interest is not an offence under French law. On the other hand, it is the fraudulent use that could result from such a situation that can be sanctioned (illegal taking of interest, favouritism, bribery, etc.).

SOME EXAMPLES OF AT-RISK SITUATIONS

- ➢ Holding an elective mandate.
- ➢ Working in any form/being in a personal business relationship with or having a significant interest in a customer, supplier or competitor of the Group.
- ➢ Receiving, directly or indirectly, advances, loans, guarantees or services, gifts, with the aim of influencing a Group decision.
- ➢ Doing business on behalf of the Group with a family member or a company with which the employee and/or a family member is associated.

GOOD PRACTICE AND PERMITTED BEHAVIOUR

- ✓ Inform your line management if activities are likely to create a conflict of interest.
- ✓ Ensure that its actions and decisions are not influenced by interests that might reasonably appear to conflict with those of the Group.
- ✓ In the event of a potential conflict of interest situation, consider whether his or her personal interests could interfere with those of the Group and whether this could be perceived as such by anyone inside or outside the Group.
- ✓ Inform your hierarchy and the HRD if you hold an elected office, a social mandate, a consultancy function, or if you hold a position of responsibility with a competitor or partner.
- ✓ In case of doubt about the existence of a conflict of interest, refer to the Internal Control and Compliance Department.

TYPES OF PRACTICES AND BEHAVIOURS THAT ARE PROHIBITED

- ✗ Influencing the hiring, job evaluation or remuneration of a relative.
- ✗ Misuse of the Group's influence and resources.
- ✗ Retaining, or helping to retain, an entity in which we or someone close to us has an interest for a contract.
- ✗ Using or sharing confidential information about the Group for our own benefit or for the benefit of a relative.
- ✗ Using the Group's partner companies for personal contracts on terms other than those applicable to the general public.
- ✗ Withholding information on any conflict of interest, even potential conflicts.

You can also consult the Sodiaal Group's ethical commitments in the duty of care plan, published annually in the framework of the so-called "duty of care" law (2017).

VI

PROCESSING PERSONAL DATA

1.Processing personal data

Personal data (PDS) is a very broad concept that encompasses any information relating to an identified or identifiable natural person.

There are 2 types of identification:

- direct identification (surname, first name etc.);
- indirect identification (ID, number etc.)

The Sodiaal group undertakes to respect the rules applicable in the area of personal data protection, both with regard to its producers, employees and third parties, in particular customers, suppliers and consumers, and to comply with the legal requirements in this area.

The Sodiaal Group has appointed a Data Protection Officer (DPO) and has put in place a personal data protection system that complies with the requirements of the GDPR (General Data Protection Regulation) including:

- Monitoring of data processing, in order to identify and list existing processing operations and to keep an exhaustive inventory of them.
- Information on the rights of the persons concerned by the processing of personal data (information on the nature and purpose of the processing operations concerning them, on the procedures for exercising their rights and on the methods for obtaining consent).
- The updating of the relevant contracts.
- An e-learning programme.

Each employee of the Sodiaal Group is obliged to comply with the rules and mechanisms in place:

- Do not save files containing personal data on the hard disk or USB stick.
- Do not take personal data outside the company.

2.GDPR best practice rules

WHEN COLLECTING PERSONAL DATA

TO BE DONE

- ✓ Precisely identify the initial purposes of collecting personal data to make them determined and explicit.
- ✓ Examine the formalities carried out for the processing and the disclosure statements to determine whether the purposes for collecting and processing personal data are identified and explicit.
- ✓ Analyse the legitimacy of the purposes for collecting and processing personal data.

WHAT NOT TO DO

- ✗ Collecting personal data where its origin is unknown to the controller.
- ✗ Processing prohibited personal data (health, religion, political opinions, etc.).
- ✗ Collecting personal data without informing individuals about the purposes of collecting and processing of personal data.
- ✗ Using a processing operation for other purposes without considering the compatibility of these new purposes with the original purposes.

QUALITY OF PERSONAL DATA

TO BE DONE

- ✓ Periodically update personal data processing and files.
- ✓ For free comment fields, ensure that only personal data necessary for processing are collected.

WHAT NOT TO DO

- ✗ In the free comment fields:
  - personal judgements, value judgements: abusive, derogatory, hurtful expressions;
  - Assessments of the person's character (e.g. 'shy person', 'bad character', etc.);
- ✗ Personal data on racial, ethnic origin, political, religious, philosophical opinions, trade union membership, health, sex life.

PERSONAL DATA RETENTION PERIOD

TO BE DONE

- ✓ Check that there are retention periods for each category of personal data processed within the processing operation.
- ✓ Assessing the retention period in relation to the purpose of the data.

WHAT NOT TO DO

- ✗ Extracting data from an application and retaining that file without ensuring that the original retention period is respected.
- ✗ Encouraging or facilitating Excel extractions.
- ✗ Do not define a shelf life in applications during the development phase.

RECIPIENTS OF THE PROCESSING OPERATIONS

TO BE DONE

- ✓ Identify the recipients of each processing operation with reference to the formality carried out beforehand.

WHAT NOT TO DO

- ✗ Communicating personal data to third parties without checking their clearance.

TRANSFERS OF PERSONAL DATA

TO BE DONE

- ✓ Identify transfers made outside the European Union.
- ✓ Check which legal framework the transfer to the identified countries is subject to.

WHAT NOT TO DO

- ✗ Implementing data transfers to countries outside the European Union that do not have adequate protection without a legal framework.

INFORMING DATA SUBJECTS

TO BE DONE

- ✓ Ensure that data subjects have been informed of the processing that is going to be carried out. Where appropriate, inform the data subjects by means of a notice.

WHAT NOT TO DO

- ✗ ✗ Not including a notice or including it in such a way that it is not easily visible.

VII
RIGHT TO DISCONNECT

The development of digital technology has led to changes in the working environment and conditions. While information and communication technologies make exchanges more fluid, improve productivity and break down spatial barriers, excessive use can lead to risks for employees. The constant demands of these new modes of communication during working hours cause information overload, create a sense of urgency and stress, and lead to a growing encroachment of work life into the private life of the employee outside working hours.

In this context, the Sodiaal Group is committed to supporting employees in the proper use of digital tools to improve the quality of life at work and reaffirms the importance of respecting the balance between private and professional life by guaranteeing the right to disconnect during rest time.

It is understood that not all of the following provisions are intended to be applied:

- To senior managers
- To employees on call
- To employees travelling abroad on business or in contact with foreign countries

1. Right to disconnect for all outside normal working hours

In order to preserve the balance between professional and private life, the Sodiaal group reaffirms that rest periods (11 hours daily and 35 hours weekly), holiday periods and suspension of the employment contract must be respected by all the stakeholders of the Sodiaal group.

To this end, the Group recognises a right to disconnect for each employee, which translates into the right not to be connected to professional digital tools and not to be contacted, including on their personal communication tools, for a professional reason outside their usual working hours and during their paid holidays, rest periods and absences, whatever their nature. No employee may be sanctioned for using his or her right to disconnect.

The use of digital tools outside working hours must be justified by the urgency or importance of the subject matter.

2. Managers and executives leading by example

Line management will ensure that the right to disconnect is respected by leading by example. Managers should pay particular attention to the balance between the professional and private spheres of the employees under their supervision by ensuring that they do not send e-mails outside normal working hours.

The Sodiaal group undertakes to make the right to disconnect a compulsory theme of the annual appraisal interviews or, for managers subject to a fixed number of days agreement, of the workload interviews.

BEST PRACTICE RULES FOR A REASONABLE USE OF PROFESSIONAL DIGITAL TOOLS

DURING WORKING TIME TO IMPROVE THE QUALITY OF LIFE AT WORK

- ✓ During meetings, limit the use of the PC and telephone as much as possible;
- ✓ Question the functions of the different communication tools according to the purpose: emails, phone, Jabber, My Universe…
- ✓ Prefer physical meetings to sending emails in order to encourage interaction;
- ✓ Ensure that the recipients of the email are appropriate and that the "Reply All" and "Copy to" functions are used sparingly;
- ✓ Make sure that the subject line of the email is precise, as this subject line should allow the recipient to immediately identify the content of the email;
- ✓ Avoid writing "Urgent" and do not request an immediate response when not necessary;

OUTSIDE WORKING HOURS TO ACHIEVE WORK-LIFE BALANCE

- ✓ Ensure that the use of professional tools outside working hours is moderate, in particular in order to respect the mandatory rest periods of 11 hours per day and 35 hours per week;
- ✓ Consider when to send an email/SMS or call a colleague on their work phone to avoid creating a sense of urgency;
- ✓ Choose to send an email later when writing an email outside working hours;
- ✓ Set up the "out-of-office manager" on the email and provide emergency contact details;
- ✓ Alert line management in the event of recurrent excesses;
- ✓ Mention in emails "if you receive this message outside your normal working hours you are not required to respond immediately".
- ✓ Ensure neutral, clear and concise emails are sent.

VIII

RULES FOR THE USE OF COMPUTER AND DIGITAL RESOURCES

1.Group commitment to information security

These provisions aim to preserve the Sodiaal group's IT system, in compliance with the legal and regulatory obligations in force.

The Group implements a comprehensive security system for its IT system against both external and internal malicious acts.

It is reminded that each user (internal or external employee (permanent or fixed-term contract, external service providers, trainees, temporary workers, etc.) is directly responsible for the use of the information and communication resources to which he or she has access. He or she is responsible, at his or her level, for contributing to general safety.

2. Role and responsibilities of users of IT and digital resources

The use of IT and digital resources is intended for the needs of the employees' professional activity.

As such, these resources may be deleted, suspended or restricted, particularly in terms of volume (connection time, email size, available bandwidth, attachment files, disk space quota, etc.) individually or collectively when necessary and particularly to maintain the proper functioning and integrity of the company's resources.

Users undertake to:

> Respect the laws and regulations in force; in particular, the following are prohibited:
  1. attempts to illegally intrude on a system,
  2. access to resources to which he or she is not entitled,
  3. viewing
  4. disseminating political, racial or religious ideologies, or which are of a nature to undermine public order, good morals, dignity, honour or the private life of individuals.

> Have a non-abusive use of the computer and digital tools to which they have access.

Non-abusive use is defined as use within the framework of the necessities of daily and family life, remaining reasonable and reasoned and complying with these rules and regulations.

For personal use, the user assumes full responsibility and all possible legal and financial consequences.

> Comply with security measures relating to computer and digital resources.
> Respect the equipment, software and tools provided to them as well as the technical notes and instructions for their use.
> Respect the confidentiality of the data exchanged and processed.
> Notify any malfunction or fraudulent use of computer and telephone tools, as well as of any loss or theft, as soon as possible.
> In no way lead to the company's image being called into question.
> In no way hinder or limit the professional use of these resources, their maintenance or their security.
> In no way hinder or delay the deactivation of an outgoing employee's or contractor's access.
> Not introduce any equipment on the network that is not supplied by the Information Systems Department unless explicitly and formally authorised.
> Not use the resources made available to them for profit-making or recreational activities.

A. SYSTEM ACCESS MANAGEMENT

IDs:

Users are responsible for their use of the Group's IT and telephone tools.

A unique and personal ID (login and password) is given to each user. This restriction aims to identify anyone using a computer. This ID allows the user, at each connection, to be assigned specific rights and privileges on the system resources he or she needs for his or her activity.

The user is therefore personally responsible for the use that may be made of it and must not under any circumstances communicate it. These operations are automatically traced at different levels in the application logs. These logs are stored by the company under the conditions recommended by the CNIL (French Data Protection Agency).

The company can use these traces as evidence of the employee's actions and, in the event of use that may constitute a nuisance, they can be used to establish proof of this.

No-one has the right to impersonate another person or to act anonymously.

Similarly, holders of accounts or access control devices are responsible for transactions carried out from their accounts or under the cover of the access control devices allocated to them.

In general, users must take all measures to prevent fraudulent access to computer and telephone tools and, in this respect, they must in particular:

✓ Anticipate the departure of their employees or attached service providers in order to make the management of departures more fluid ("Checkout").
✓ Ensure the confidentiality of user accounts assigned to them.
✓ Not lend, sell or transfer user accounts, codes or access control devices or pass them on to a third party.
✓ Log off after their period of work on the network has ended or when they are away.
✓ Inform the IT manager of any attempted fraudulent access or suspicious malfunction.
✓ Ensure that files they consider confidential or classified as confidential are not accessible to unauthorised third parties.
✓ Ensure that their PCs are put into lockdown mode during partial absences during the day, and that the security cable is attached for laptops.

These IDs will be locked after the employee has left (a comparable mechanism governs the departure of service providers; every partner manager must be involved in this management).

It is also specified that the user's access to computer or digital resources may be suspended, limited or reviewed for security reasons, in particular:

> When the employee ceases to work in his or her department or company (change of department, transfer, etc.)
> In certain cases of temporary cessation of professional activity (sick leave, maternity leave, etc.)

> As soon as illicit or abusive use (breaches of the present regulations, etc.) is suspected or demonstrated

Remote access (via VPN) :

The Sodiaal group provides mobile users with a VPN access that allows them to work on the company network from their professional computer outside the company and connected to the Internet. These configurations require particular diligence:

The VPN connection is mandatory when the user uses a public network (train station, hotel lobby, airport, etc.) in order to secure communications.
Disconnection from the VPN is mandatory as soon as the user leaves the workstation.
The password should never be disclosed.

Specific characteristics related to mobile working

Only authorised users can connect a mobile working tool to the company network.
No computer or mobile working tool not entrusted or approved by the Company should be connected to the company network without the explicit authorisation of the ISSM.
Any mobile working tool approved by the Company may be subject to any one-off or permanent security check organised by the ISSM.
In this respect, the holder of the mobile working tool concerned discharges the Company of any responsibility for any prejudicial consequences linked to these checks (deletion of data, malfunction, etc.).

B. RULES FOR THE PROPER USE OF THE RESOURCES MADE AVAILABLE

General points:

The use of the equipment provided is subject to prior authorisation by the line manager, and may be withdrawn at any time in the event of non-compliance with the Sodiaal code of conduct.

The user undertakes to use this equipment only for professional purposes. S/he will take particular care of his physical safety, especially in vehicles (temperature, theft) and in public places.

The personal use of the computer equipment entrusted to him or her is tolerated by the Management as long as this use does not disrupt the professional activity of the company and does not generate significant additional costs (and on an exceptional basis). In the event of abuse, the company may have to carry out checks.

However, it should be noted that in order to guarantee the security of the systems, only an administrator is authorised to introduce new hardware and software. As such, the following are prohibited unless explicitly authorised by the IT services

- ✗ Downloading, installing and using software.
- ✗ The introduction of equipment (computer, phone, tablet, etc.) not provided by the Information Systems Department onto the network.

The employee must inform the company immediately in the event of malfunction, theft* or blockage of the computer equipment.
** In addition, any theft of equipment must be reported to the local gendarmerie or national police. It will be forwarded to the IT asset manager and the Group's Data Protection Officer (DPO): Annabel Francony Legros annabe.legros@sodiaal.fr/01 44 10 90 71).*
In the event of contact or a prolonged stay abroad outside the European Union, the user should contact his or her telephone contact person in order to adapt the tariffs as best as possible.

Respect of intellectual property rights:

It is strictly forbidden to copy software for any purpose whatsoever. All software implemented at the Company must be used and operated in accordance with its licence and subject to the necessary permissions.
The same applies to all works such as photographs, images, databases, audiovisual and musical works, texts, etc. protected by copyright. In particular, the User must not use the Resources made available by the Company to infringe intellectual property rights and in particular copyright (illicit downloading or

unauthorised sharing of works protected by copyright, etc.).

Specifics related to electronic messaging:

E-mail is provided by the company for professional exchanges. The data conveyed by the message flows may be kept under the conditions recommended by the CNIL for inspection purposes.

Every user should be aware that a message sent over the Internet can potentially:

- Be malicious (phishing, fraud, etc.)
- Be intercepted, even illegally, and read by anyone.

An e-mail object (messages, appointments, address book, tasks, etc.) stored in the e-mail system by an employee may be private, especially when synchronised with a mobile phone.

It is up to the employee to identify the objects that are personal to him or her by setting the value "Private" in the "Distribution Criteria" list in the "Property" menu of the object.

Reasonable private use, particularly in terms of number and volume, is tolerated within the context of the requirements of everyday life and family life, provided that the use of electronic mail does not affect the normal traffic of professional messages or disrupt the professional activity of the user. It is the employee's responsibility to inform his or her private correspondents so that they explicitly identify the private nature of their message in the subject line of their e-mails.

The content of those explicitly indicated as being of a private nature may not be accessed by the company without the user's express authorisation, but a statistical check may be carried out in order to evaluate the possible sensitivity or danger for the company and its network.
In the absence of such identification, messages are presumed to be professional.

When using their professional e-mail, users must ensure that they:

- ✗ Remain vigilant on a daily basis in the face of fraudulent or malicious messages (phishing) of any kind (request for confidential information such as passwords, booby-trapped attachments, transfer fraud, etc.) and to notify their manager and the IT department in the event of doubt or action(s) carried out inadvertently.
- ✗ Do not disseminate information outside the company about the professional activity, mission, projects, relations within the group, or any confidential information that could be used by a third party for business intelligence or malicious purposes.
- ✗ Do not participate in chain letters.
- ✗ Do not denigrate or defame the company, its competitors or anyone else
- ✗ Do not communicate in an offensive way about the race, sex, religion, political opinions, social origins, age or disability, of a third party.
- ✗ Do not convey illicit content (pornography, paedophilia and any degrading behaviour).
- ✗ Prohibit any sexual or moral harassment.
- ✗ Refrain from any action that may engage the civil or criminal liability of the company.

Specifics related to corporate Internet browsing:

Users must use Internet services in accordance with the general principles and rules of the various sites and in compliance with the legislation in force.
Occasional use of the Internet for private purposes is tolerated within reasonable limits, provided that browsing does not interfere with professional access or disrupt professional activity.

It is the criminal and ethical responsibility of the company to prohibit the consultation of any legally prohibited site, in particular those of a pornographic, paedophilic, incitement to racial hatred or revisionist nature, etc.

For this reason, a system for filtering unauthorised sites (sites disseminating pornographic, paedophilic, incitement to racial hatred, revisionist, etc.) is administered by the IT department.

As no system guarantees a total filter, an additional mechanism allows detailed analysis of Internet browsing history. This history is stored for the legal period in force and analysed periodically.

In addition, users shall ensure that they do not use the company's Internet or company email address for the purpose of:

- ✗ Participating in non-professional forums and/or social networks.
- ✗ Creating personal web pages.
- ✗ Carrying out a personal business activity or clandestine work.
- ✗ Attempted breach of computer system access.
- ✗ Illegal activities or activities contrary to internal rules.
- ✗ Denigration or defamation of the company, its competitors or anyone else.
- ✗ Games or actions aimed at obtaining personal profit or gain.
- ✗ Offensive communication relating to race, sex, religion, political opinion, social origin, age or disability.
- ✗ Sexual or moral harassment
- ✗ Any action that may give rise to liability.
- ✗ Paedophilia, pornography, incitement to racial hatred, revisionist statements, etc.)

Specifics related to common or individual storage/sharing spaces:

As a matter of principle, any data storage/sharing space is made available by the company for the exclusive purpose of storing business information. Private data may exceptionally be stored on an individual space, provided that the disk space used for this data is limited and that this data is grouped in a folder called "Personal data". If this is not explicitly named, these data may be considered as the property of the company, and therefore available for viewing.

The shared network space may not contain any data other than business data.

The Information Systems Department reserves the right to demand the deletion of such data from shared networks if their owner can be identified, or failing that to delete them.

3.Role and responsibility of administrators

An IT Administration Charter supplements the User Charter and applies to all users of the group and more specifically to those with administrator status.
It aims to:

- **Avoid any form of abuse of the use of IT tools and constitutes a binding reference document within Sodiaal.**
- **Specify the rights and duties of the Administrator in the exercise of his or her function or professional activity.**

A. GENERAL POINTS

Administrators are responsible for ensuring the normal operation and security of networks and systems.
By virtue of their very functions and as an exception, they are the only ones to have access to personal information relating to users (e-mail, history of sites visited, "log" or logging files, etc.), including those recorded on the workstation's hard disk (temporary files, cookies, etc.).

B. ACCESS TO USERS' PERSONAL DATA BY IT ADMINISTRATORS

Access to data recorded by employees in their IT environment - which may be of a personal nature - can only be justified in cases where the proper functioning of IT systems could not be ensured by other, less intrusive means.
Similarly, network and system administrators must not divulge information that they may have come to know in the course of their duties, in particular when such information is covered by the secrecy of correspondence or concerns the private lives of users and does not jeopardise the proper technical functioning of applications, their security or the interests of the company. Nor can they be compelled to do so, unless specifically provided for by law.

C. THE USE OF REMOTE CONTROL SOFTWARE

In particular, remote control software can allow technical managers to remotely access all data on any workstation for IT maintenance purposes.
If these tools are used for computer maintenance purposes by a technical administrator, their use must be surrounded by precautions to guarantee transparency in their use and the confidentiality of the data to which the technical manager will have access by this means, within the strict limits of his or her needs.

> The user must be informed in advance and consent must be obtained to "authorise the hand" of the IT administrator before any intervention on his or her workstation. By way of illustration, consent can be given by simply validating an information message that appears on screen.

✗ The use of remote maintenance or remote control tools for the purpose of monitoring, by the employer, the activity of its employees on their computer workstations is prohibited, as it is neither in accordance with the principle of proportionality nor respectful of the principle of purpose laid down by the French "Data Protection" Act.

D. BUSINESS CONTINUITY

Where continuity of service requires it, administrators may need to take the necessary steps to access the resources made available to the absent or prevented User, for example to establish or re-establish delegations of access or to put in place appropriate absence managers.
Any administrator who is given access to these resources is informed that he or she must respect the secrecy of private correspondence and that he or she is forbidden to take cognizance of any personal content, on pain of being held liable.
Any user who is absent is informed in advance of the nature of the intervention, except in cases where this is impossible (unplanned absence).
In order to keep this type of procedure exceptional, it is important to work and store files on shared spaces in order to facilitate access to professional files for authorised persons.
The deletion or attempted deletion by the user of any information useful to the company's activity may be considered as wrongful. Furthermore, in the event of departure from the company, files or messages of a private nature which have not been deleted by the user may be deleted by the company, the others will be deemed to belong to the company and kept as such.

4.Checking and traceability

For the purposes of security and verification of proper access to and use of IT and digital resources, as well as the proper functioning of the Information System, the Information Systems Department implements filtering and control systems (firewalls, access control systems, etc.).
These systems can be implemented to control any incoming or outgoing electronic message (antiviral control, antispam control, size control, list of recipients, etc.) and also to block, notably on the basis of a list of keywords, messages, computer exchanges or access to unauthorised sites.
They record the various history of activity of the Resources, for the purposes of Information Systems security.

In accordance with the principles of transparency and proportionality, the User is informed that the following records are kept:

- list of content or services to which the User has had access on the Internet or Intranet;
- in general, a list of technical parameters for managing access/connection or attempted access/connection to any internal or external communication network from critical resources (telephone network, Internet, internal networks, etc.), size and type of files accessed, etc.;
- list of technical parameters for the management of electronic messaging services (user account identification, recipient details, date and time, etc.).

For statistical purposes relating to connections and exchanges, the ISSM may carry out checks on the volume of log-ons to Internet sites or on the use of e-mail.
A posteriori checks may therefore be carried out on the volume of visits to Internet sites or

use of the e-mail system: a record of the most visited sites, of the user accounts that have generated the most requests (hits), a record - for these - of the duration of visits and of the most frequented sites, etc.

✗ The User shall not in any way prevent or hinder the normal operation of these checking means.

If necessary, and depending on the results of the checks carried out, certain resources (non-professional sites visited from the Company's network, etc.) may be restricted or even prohibited by the Information Systems Department without prior notice or information.

The User is informed that individualised checks may be carried out by the ISSM following a malfunction of the Resources, a security alert (prevention of data leakage or violation of personal data, etc.) and also in the event of suspected non-compliant use of these Resources, subject to compliance with the provisions applicable to the confidentiality of private correspondence.
In this context, the purpose of the material findings is to identify the various circumstances that will shed light on the possible occurrence of an incident and its origin, in order to take all appropriate measures, if necessary by implementing disciplinary and, if necessary, legal procedures.

Any breach of the provisions of the code of conduct may be subject to disciplinary action and/or criminal proceedings (for temporary or external staff, disciplinary proceedings will be the responsibility of the company to which they belong).

IX
ETHICS ALERT

LET'S TALK ABOUT IT TOGETHER

All of us, regardless of our position or role, have the right to speak out about situations of concern. We all have a responsibility to report the facts and express our concerns in a fair, honest and professional manner.

This system offers internal, external and occasional employees an alternative means of reporting non-compliance situations to line management or to the Internal Control and Compliance Department.

The whistleblowing procedure must allow for the collection of any report or disclosure made in a disinterested manner and in good faith: a crime or offence; a serious and manifest violation of an international commitment regularly ratified or approved by France; a serious and manifest violation of a unilateral act of an international organisation taken on the basis of an international commitment regularly ratified or approved by France; a serious and manifest violation of the law or regulations; a serious threat or prejudice to the general interest of which the whistleblower has personal knowledge; relating to the obligations defined by European regulations and by the monetary or financial code or the general regulations of the *Autorité des marchés financiers*, and whose supervision is ensured by the *Autorité des marchés financiers* or the *Autorité de contrôle prudentiel et de résolution*; relating to the existence of conduct or situations contrary to the company's code of conduct, concerning acts of corruption or influence peddling, provided that the implementation of these processing operations responds to a legal obligation or legitimate interest of the data controller.

HOW DO WE ALERT

>Alert telephone number: 0800 94 16 50

> Alert e-mail address: conformite@groupesodiaal.fr

WHISTLEBLOWER PROTECTION

The Sodiaal Group undertakes to protect its employees who signal an alert via this system against any reprisals, provided that they act in good faith.

However, if the warning system is used with the intention of harming others, the whistleblower may be sanctioned by the Sodiaal group or may be subject to legal proceedings.

WHAT IS RETALIATION?

By retaliation we mean any action, whether direct or covert, that illegitimately sanctions an employee for reporting an actual or suspected situation of concern in good faith.

Retaliation is a serious breach that the Sodiaal Group will not tolerate, and any employee resorting to it may be sanctioned.

CONFIDENTIALITY

Any situation reported under this whistleblowing scheme will be treated impartially and confidentially

Date of the update of the code of conduct: September 2021.