WHISTLEBLOWING POLICY AND PROCEDURES

Contents

GENERAL POLICY PURPOSE AND APPLICATION

The CLN Group policy (the **Policy**) is approved and adopted by the Board of Directors of each CLN Group Company and will be revised at least every 12 months to ensure its adequacy and effective implementation.

The Policy consists of three sections:

Section 1

Section 1 applies to all CLN Group Companies (based in the EU and outside the EU) with a wide application and scope, aiming at providing an avenue to report concerns about corporate conduct for a broad range of parties, including employees, suppliers, and business partners. Section 1 must be adopted by all CLN Group Companies.

Section 2

Section 2 complies with EU Directive 2019/1937 (also known as the "Whistleblowing Directive") and consequently applies only to CLN Group Companies based in EU Countries that have put the Whistleblowing Directive in a local law. Section 2 must be adopted only by CLN Group Companies based in EU Countries and should be read in the light of paragraph 5, which offers a detailed explanation of the local laws' peculiarities and obligations.

Section 3

Section 3 complies with Brasil law 13.709/2018 and applies only to CLN Group Companies based in Brasil.

SECTION 1

1. PURPOSE

In addition to local legal requirements, CLN Group is committed to the highest possible standards of ethical, moral, and legal business conduct through the ethical behaviour of its employees and the proper and effective functioning of its accounting and control systems. In keeping with this commitment, and the commitment to open communication and transparency, this Policy aims to provide an avenue for employees and other external parties to report concerns, with the reassurance that they will be protected from reprisals or victimization for whistleblowing in good faith.

2. POLICY APPLICATION

Section 1 of this Policy applies to internal Stakeholders such as all CLN Group employees worldwide (including part time, temporary and contract employees), shareholders and joint venture partners.

Section 1 can also be used by external Stakeholders such as employee family members, customers, suppliers, contractors, business partners, local communities, and other connected parties, to report any concerns about our business practices or conduct.

3. POLICY SCOPE

Section 1 is intended to cover serious concerns regarding human rights, the environment, information security or unethical business practices such as bribery, corruption or anti-competitive acts that could have a large impact on the CLN Group, such as actions that:

could lead to incorrect financial reporting.

are unlawful.

are not in line with the CLN Group's policies and Code of Ethics.

otherwise amount to serious improper conduct.

Disputes, claims or requests linked to the personal interest of the person making the claim that relate exclusively to his/her individual employment relationships, or inherent to his/her employment relationships with superiors, or relate to local salary and/or conditions negotiations cannot be reported. Such issues should be discussed with the local human resources department.

4. POLICY PROCEDURES

4.1 Confidentiality

A complainant's identity will be kept confidential unless that person has authorized its disclosure in writing.

4.2 Anonymous reports

Employees are encouraged to put their names to allegations as appropriate follow-up questions and investigation may not be possible unless the source of the information is identified. Concerns expressed anonymously will be investigated, but consideration will be given to:

the seriousness of the issue.

the amount of detail provided.

the credibility of the concern.

the likelihood of confirming the allegation from other sources.

4.3 Whistleblower protection against retaliation

Complainants will be protected against harassment, retaliation or victimization for reporting concerns and complaints in good faith under this Policy. Any such actions against the complainant will not be tolerated and will result in disciplinary action up to and including termination.

This also means that the continued employment and opportunities for future career progression or training of the employee will not be prejudiced because he/she raised a legitimate concern.

4.4 Malicious allegations and self-disclosure

Malicious allegations may result in disciplinary action. The Policy will not protect a person from the consequences of his or her own wrongdoing; however, a person's self-disclosure of wrongdoing that has not previously been independently discovered through investigation will be considered when considering the consequences to such a person.

5. PROCEDURES FOR REPORTING CONCERNS AND COMPLAINT

The whistleblower procedure is intended to be used only for serious and sensitive issues. Minor issues should be reported to local management.

CLN has established a confidential and anonymous process to receive complaints.

Serious concerns relating to unethical or illegal conduct can be reported to the Group platform (https://leaks.gruppocln.com). If the complainant is not able or willing to use the Group platform, a complaint can also be sent to the email a.gordon@gruppocln.com and it will be forwarded to the Whistleblowing Committee. A complainant may also request a video-call meeting with a member of the Whistleblowing Committee, which will be set within 30 days.

5.1 Evidence

Although the complainant is not expected to prove the truth of an allegation, he or she needs to demonstrate that there are sufficient grounds for concern.

6. HOW THE COMPLAINT WILL BE HANDLED

6.1 Whistleblowing Committee

The responsibility for investigating and handling reported complaints and allegations is delegated to the Whistleblowing Committee. The Whistleblowing Committee comprises three members, two of them being senior executives of CLN and one being an external person not employed in CLN Group. The members of the Whistleblower Committee have been chosen by the Group CEO because they are competent, impartial and independent of the day to day running of the Group's operations.

The Whistleblowing Committee will receive, retain, investigate, and act on all complaints and concerns. The action taken will depend on the nature and the severity of the concern. All complaints and concerns received through the Group platform or through other communication methods will promptly be assessed by the Whistleblowing Committee, who will decide and report on how each complaint is handled and the action taken.

6.2 Report to complainant

The complainant will receive the following information within a reasonable time frame:

Acknowledgement that the complaint was received.

Indication as to how the matter will be dealt with and further consultation with the complainant where required.

An estimate of the time that it will take for a final response.

Status of investigation.

Final conclusions and action taken.

In the case that the complainant is not happy with the final conclusions and action taken and wants to appeal accordingly, he/she can do so by emailing a.gordon@gruppocln.com. Appeals of this nature will be forwarded to the Group CEO, together with a report from the Whistleblower Committee on the complaint, who will determine if the appeal justifies further steps to be taken.

SECTION 2

1. PURPOSE

CLN Group has implemented a whistleblowing system in accordance with the requirements of the Whistleblowing Directive and local laws implementing it. This Policy applies to CLN Group Companies based in an EU Country that has adopted a local law which implements the Whistleblowing Directive.

2. PROCEDURES

2.1 Definitions

Company/Companies	Companies of CLN Group based in an EU Country that has adopted a local law implementing the Whistleblowing Directive
Country	EU Country that has adopted a local law implementing the Whistleblowing Directive
Facilitator	A natural person who assists a reporting person in the reporting process, operating within the same working environment and whose assistance must be kept confidential
Feedback	The provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up
Follow-up	Any action taken by the recipient of a report to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure
Group	The CLN Group
Policy	The global whistleblowing policy adopted by the Group and applied worldwide
Guidelines	Guidelines on the local whistleblowing discipline adopted by a Country public authority
Information on breaches	Information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organization in which the reporting person works or has worked, and about attempts to conceal such breaches
Person concerned	The natural or legal person named in the report as the person to whom the breach is attributed or as a person otherwise involved in the reported breach
Reporting person	The natural person reporting Information on Breaches acquired within his or her work-related context

Retaliation	Any conduct, act, or omission, even if only attempted or threatened, engaged in by reason of the report and which causes or may cause unjustified detriment, directly or indirectly, to the reporting person
Breaches	Acts or omissions damaging the public interest or the integrity of the Company
Work-related context	Current or past work or professional activities through which, regardless of the nature of those activities, a person acquires Information on breaches and within which he/she could risk retaliation in the event of a report
EU Directive 2019/1937	Whistleblowing Directive
GDPR	Regulation (EU) 2016/679 - General Data Protection Regulation

2.2 Breaches that can be reported

Reports may be made with respect to certain matters. In general:

(1) Breaches falling within the scope of the European Union acts listed in the Annex to the Whistleblowing Directive and any national law implementing it. These offences relate to the following areas:

- public procurement;
- financial services, products and markets and prevention of money laundering and terrorist financing;
- product safety and compliance;
- transport safety;
- protection of the environment;
- radiation protection and nuclear safety;
- food and feed safety, animal health and welfare;
- public health;
- consumer protection;
- protection of privacy and personal data, and security of network and information systems.

(2) Breaches affecting the financial interests of the European Union (Art. 325 TFEU, fight against fraud and illegal activities affecting the financial interests of the European Union) as identified in Union regulations, directives, decisions, recommendations, and opinions (e.g., fraud, corruption and any other illegal activities related to Union expenses)

(3) Breaches relating to the internal market that jeopardize the free movement of goods, persons, services, and capital. This includes Breaches of Union competition and state aid rules, corporate tax

rules and mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law

(4) Breaches that frustrate the object or purpose of Union acts in the areas mentioned in the preceding bullet points.

Local laws may provide for additional and further matters that may be subject to reporting, please refer to paragraph 5.

2.3 Breaches that cannot be reported

Disputes, claims or requests linked to a personal interest of the Reporting person that relate exclusively to his/her individual employment relationships, or inherent to his/her employment relationships with superiors, cannot be reported.

However, please note that the reasons that led the person to report are irrelevant for the purposes of processing the report and of protection from retaliatory measures.

2.4 Elements and characteristics of the report

Reports should be as detailed as possible to allow the evaluation of the facts by the competent entities receiving and managing them (e.g., circumstances of time and place, description of the facts, personal details or other elements that allow the identification of the person(s) involved in the report).

It is also useful to attach documents that can provide evidence of the reported facts, as well as an indication of other people potentially aware of the facts.

2.5 Persons who can make reports

The following persons may report Breaches as referred to in paragraph 2.2:

(A) employees, including workers with fixed-term, part-time or intermittent contract, apprenticeship, and occasional workers;

(B) self-employed workers carrying out intellectual professions registered in special registers or lists (e.g., architects, engineers, surveyors); holders of a collaboration relationship such as agency, representation or other coordinated and continuous collaboration relationships; holders of collaboration relationships organized by the client that result in exclusively personal and continuous work services;

(C) freelancers and consultants working for the Company (excluding lawyers and doctors who are bound to professional secrecy);

(D) volunteers and trainees, paid and unpaid, who work at the Company;

(E) shareholders;

(F) persons with administrative, management, control, supervisory or representative functions, also *de facto*, such as directors, auditors, members of Supervisory Body *ex* Decree no. 231).

The protection also applies during the probationary period and before or after the establishment of the employment or legal relationship, and when:

the described legal relationship has not yet begun, if the Information on breaches was acquired during the selection process or in other pre-contractual stages;

during the probationary period;

after termination of the legal relationship if the Information on breaches was acquired during the same legal relationship.

2.6 Internal reports

(a) Internal reporting channel

CLN Group, also informing union representatives, has created an internal reporting channel which guarantees the confidentiality of the identity of the Reporting person, the Facilitator, the Person involved, and any person mentioned in the report, the content of the report and the related documentation.

The management of the reporting channel is entrusted to the Whistleblowing Committee, that meets the requirements of autonomy, independence and competence requested by the law.

Reports are made in written form through the Group platform (https://leaks.gruppocln.com) or orally in a video-call meeting with a member of the Whistleblowing Committee, for which is necessary to send a request of email with an email to a.gordon@gruppocln.com. The meeting will be set within 30 days.

Reports from which the Reporting person's identity cannot be established are considered anonymous. Anonymous reports, where detailed, are to be considered and managed as ordinary reports.

(b) Handling of internal reporting channel

The Whistleblowing Committee carries out the following activities:

(A) gives the Reporting person notice of receipt of the report within 7 days of that receipt;

(B) if requested, sets a face-to-face or video-call meeting with the Reporting person within 30 days;

(C) maintains contact with the Reporting person and requests additional information, if necessary;

(D) assesses the existence of the essential requirements of the report to determine its admissibility and be able to grant the Reporting person the protection prescribed and diligently follows up the reports received;

(E) gives the Person concerned the opportunity to be heard upon request, or, when deemed appropriate, through a written procedure by acquiring written observations and documents;

(F) provides a response to the report within 3 months from the date of the acknowledgement of receipt or, if no such acknowledgement is received, within 3 months from the expiration of the 7-day period from the submission of the report.

The report may be deemed manifestly inadmissible due to, for instance, (i) the absence of factual elements relating to the Breaches that can be reported, (ii) the absence of elements capable of justifying further investigations, (iii) the minor relevance of the report.

Reports submitted to a person other than the Whistleblowing Committee should be forwarded to the Whistleblowing Committee within 7 days after receipt, with simultaneous notification provided to the Reporting person.

2.7 External report

Reporting persons can also make external reports of the Breaches listed in paragraph 2.2 to the competent public authority, designated in each Country. In general, external reporting channel provided for by the

competent public authority shall guarantee the confidentiality of the identity of the Reporting person, the Person involved, and the person mentioned in the report, as well as the content of the report and related documentation.

Please refer to paragraph 5 to know (i) a list of competent public authorities for each Country with their respective reporting channels and (ii) prerequisites for making external reports, if any, and specific rules for handling the external reports.

2.8 Protection measures

The following protection measures are guaranteed to all Reporting persons:

(1) protection of the confidentiality of the Reporting person, the Facilitator, the Person involved, and the persons mentioned in the report (paragraph 2.9);

(2) protection against any retaliatory measures taken by the Company as a consequence of the report and the conditions for their application (paragraph 2.10)

(3) limitations of liability with respect to the disclosure and dissemination of certain categories of information operating under certain conditions (paragraph 2.11)

(4) provision of support measures (paragraph 2.12).

For further information about protection measures in a specific Country, if any, please refer to paragraph 5.

2.9 Protection of confidentiality

The confidentiality of the Reporting person's identity, the Facilitator, the Person involved, and any individuals mentioned in the report is ensured throughout all stages of the reporting process.

This obligation requires that any disclosure of the Reporting person’s identity to individuals other than those competent to receive or follow up the reports should only occur with his/her explicit consent.

For further information about the protection of confidentiality applicable in a specific Country, please refer to paragraph 5.

2.7.1. Data protection

The acquisition and handling of reports is carried out in compliance with the legislation on the protection of personal data and, in particular, in accordance with the fundamental principles provided by the GDPR (e.g., data controllers, data processors and people authorized to process personal data are identified and a “privacy notice” is given to the Reporting person and others involved in the report).

The protection of personal data is ensured to the Reporting person, to the Facilitator, to the Person involved and to the persons mentioned in the report, as data subjects of the data processing.

For further information about further obligations in a specific Country, if any, please refer to paragraph 5.

2.10 Protection from retaliation

The Reporting person is protected against any Retaliation against him/her. The prohibition of Retaliation also extends to those persons who could be recipients of Retaliation, even indirectly, by reason of their role in the reporting process and/or their particular relationship with the Reporting person, e.g.: Facilitators; persons in the same Work-related context as the Reporting person and who are bound by a stable affective or kinship link; work colleagues of the Reporting person, who work in the same Work-related context and who have a current relationship with said person; entities owned by the Reporting person or the entity for which the

Reporting person works or operating in his same Work-related context.

Alleged Retaliation, even if only attempted or threatened, must be reported to the competent public authority, which is entrusted with the task of ascertaining whether it is a consequence of the report.

Here are some examples of Retaliation: dismissal, suspension, or equivalent measures, downgrading or non-promotion, job or workplace changes, reduction of salary, change of working hours, suspension of training or any restriction on access to training, negative merit notes or negative references, adoption of disciplinary measures or any other sanction, including a fine.

The application of protection from retaliation applies if (i) the Reporting person made the report on the basis of this Policy, reasonably believing that the Information on the reported Breaches is true and relevant as it falls within the objective scope of this Policy; (ii) there is a connection between the report and the act of Retaliation suffered by the Reporting person (or other persons listed right above in this paragraph).

The law establishes a reversal of the burden of proof, stating that where the Reporting person proves that he/she has made a report and that he/she has suffered Retaliation because of the report, the burden of proof is on the person who carried out such retaliatory conduct or act.

For further information about the protection from retaliation in a specific Country, please refer to paragraph 5.

2.11 Limitation of liability for Reporting persons

Where Reporting persons make a report in accordance with this Policy, they shall not be held liable for violating any restrictions on disclosure of information nor shall they incur any liability whatsoever in connection with such a report, if they had reasonable grounds to believe that such report was necessary to disclose a breach.

Reporting persons shall not incur liability for the acquisition of or access to the reported information, provided that such acquisition or access does not in itself constitute a crime. If the acquisition or access itself constitutes a crime, criminal liability under national law shall remain applicable.

For further information about the limitation of liability in a specific Country, please refer paragraph 5.

2.12 Support measures

Reporting persons can benefit from support measures, e.g., information, assistance, and advice free of charge on how to report and the protection from Retaliation offered by national and European Union regulatory provisions, the rights of the person involved, and the terms and conditions of access to legal aid.

For further information about support measures in a specific Country please refer to paragraph 5.

3. SANCTIONS

The law provides for administrative sanctions that are imposed by the competent public authority, for example (i) in case of retaliation or obstruction of reports, (ii) in case of breach of the duty of confidentiality, (iii) if the reporting system is not compliant with the law (e.g., no procedures for making and managing reports have been adopted, reports have not been followed up, etc.), (iv) if the criminal liability of the Reporting person is established, even by a first-degree judgment, for the offenses of defamation or slander, or his/her civil liability for the same offenses in cases of intentional misconduct or gross negligence.

Such conduct may also result in the application of disciplinary sanctions provided for by the Company, if any.

For further information about sanctions in a specific Country, please refer to paragraph 5.

4. DOCUMENT RETENTION AND ARCHIVING OF REPORTS

Reports and the related documentation shall be retained for as long as necessary for the processing of the report and, in any case, for a term of 5 years (or less, depending on the provisions of local laws). Retention and archiving of reports shall be handle in compliance with the confidentiality obligations set out in paragraph 2.9 and the provisions of the GDPR.

5. OBLIGATIONS AND INFORMATION UNDER LOCAL LAWS

5.1 Italy

(a) Breaches that can be reported

Companies that have adopted an organizational, control and management model pursuant to Decree no. 231/2001 can also report breaches relevant under said discipline, or breaches of 231 Model.

(b) Internal reports

All reports made should clearly state "whistleblowing report" – or other caption that makes it clear the confidentiality of the report – in the subject line.

In Italy, under the applicable law, Companies with more than 249 employees cannot share the reporting channel and its handling with other Companies. Therefore, such Companies shall provide for a local reporting channel, other and additional than the Group channel. For companies based in Italy with more than 249 employees, a local channel is provided, additional to the Group one. The local channel is handled by a nominated local Whistleblowing Officer or Committee.

(c) External reports

Competent public authority: ANAC (Autorità Nazionale Anti Corruzione).

Link to external channel: www.anticorruzione.it/whistleblowing.

Link to Guidelines: www.anticorruzione.it/-schema.linee.guida.whistleblowing.

External reports can be made through the above mentioned ANAC link, under these alternative conditions: (i) internal reporting channel is missing, inactive or non-compliant; (ii) the internal report has not been followed up; (iii) the Reporting person reasonably believes that the internal report would not be followed up or is afraid of being retaliated because of the report; (iv) the Reporting person reasonably believes that Breaches may cause an imminent or certain danger to the public interest.

(d) Data protection and protection measures

A data protection impact assessment (DPIA) is carried out on all reporting channels (both Group and local, if any).

Reporting person's identity can be revealed only with his previous written consent when, in the context of a reporting procedure or a disciplinary procedure, it is necessary and essential for the defence of the Person involved.

Protection against Retaliation does not apply in case of judicial assessment (even if not final) on (i) Reporting person's responsibility for crimes of, e.g., slander or defamation; (ii) Reporting person's civil liability resulting from intentionally providing false information with intent or gross negligence (slight negligence will not result in the loss of protection against Retaliation). Protection against Retaliation applies again if mentioned judicial assessment is not confirmed in subsequent levels of judicial review.

The burden of proof's exception does not apply to Facilitators, individuals in the same Work-related context, colleagues, or legal entities that are owned by the Reporting person, entities in which the Reporting person works, or entities operating in the same Work-related context.

Judicial authority adopts all the measures, including provisional ones, necessary to ensure the protection of the Reporting person. Waivers and settlements, if any, can only be signed in protected venues (judicial, administrative, trade union).

Reporting persons liability for acquiring/discovering Information on breaches is excluded when (i) the information is necessary for the breach to be discovered, (ii) the report is made in compliance with the Policy, (iii) the information's acquisition method is legal.

Measures of support for Reporting persons are provided by specific Third Sector entities listed on ANAC website.

(e) Sanctions

Administrative sanctions applied by ANAC: (i) euros 10.000-50.000 in case of Retaliation, or obstruction of reports, or breach of the duty of confidentiality (ii) euros 10.000-50.000 if the reporting system is not compliant with the law (e.g., no procedures for making and managing reports have been adopted, reports have not been followed up, etc.) (iv) euros 500-2.500 if a judicial assessment (even if not final) establishes Reporting person's criminal liability for defamation or slander or civil liability for the same offenses in cases of intentional misconduct or gross negligence.

The same conducts will result in disciplinary sanctions provided for by the organizational, management and control model (Legislative Decree no. 231/2001).

5.2 France

(a) Breaches that can be reported

The information must relate to facts which have occurred or for which there is a high probability that they will occur. This may include incidents of moral or sexual harassment. Facts, information, and documents relating to national defence confidentiality and medical confidentiality shall be excluded from the alert regime.

(b) External reports

The whistleblower is not required to report internally before reporting externally.

Competent public authority depending the object of the whistleblowing: DGCCRF (Direction Générale de la Concurrence, la Consommation et la Répression des Fraudes), HAS (Haute Autorité de Santé), CNIL (Commission Nationale de l'Informatique et des Libertés), DGT (Direction Général du Travail), DGEFP (Direction Générale à l'Emploi et à la Formation Professionnelle), Défenseur des droits

Link to external channel: https://www.service-public.fr/particuliers/vosdroits/R20689

Law and reference : Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, Articles 6 à 13 ; Code du Travail articles L4133-1 à L4133.4 et D4133-1 à D4133-3 et L1132-1 à L1132-4 ; Loi n°2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte - Amélioration de la protection des lanceurs d'alerte; Loi organique n°2022-400 du 21 mars 2022 visant à renforcer le rôle du Défenseur des droits en matière de signalement d'alerte - Rôle du Défenseur des droits ; Décret n°2022-1284 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte – Procédures de recueil et de traitement des signalement.

(c) Guarantee of confidentiality of identity

The confidentiality of the identity of the persons making the report, the persons concerned, and any third parties mentioned in the report is guaranteed. The elements identifying the whistleblower may not be disclosed without his agreement. In some cases, however, they may be referred to the judicial authority. Where the persons responsible for collecting or processing reports must denounce the facts gathered to the judicial authority, the information identifying the whistleblower may also be communicated to him. In this case, the whistleblower is informed.

(d) Protection against retaliation, including disciplinary measures

Protection includes any retaliatory measures that would include: (i) Suspension, layoff, termination; (ii) Demotion or refusal of promotion; (iii) Transfer of duties, change of workplace, reduction of salary; (iv) Suspension of training; (v) Negative performance assessment; (vi) Disciplinary action; (vii) Discrimination ; (viii) Non-renewal of a fixed-term or temporary employment contract.

(e) Civil and criminal irresponsibility

Where the procedure for reporting or public disclosure is followed, the beneficiaries of the protection may not be ordered to pay damages for damages caused by such reporting or public disclosure.

The whistleblower must have had reasonable grounds to believe that this procedure was necessary to safeguard threatened interests. Where the reporting or public disclosure procedure is followed, the beneficiaries of protection are not criminally responsible. This irresponsibility applies to offences that may be committed to obtain documents to prove the information reported or disclosed. However, there must not have been an offence to obtain the information itself.

5.3 Germany

(a) Breaches that can be reported:

It is possible to report breaches concerning:

1. infringements which are punishable by law,

2. infringements which are subject to a fine, insofar as the infringed regulation serves to protect life, limb or health or to protect the rights of employees or their representative bodies,

3. other infringements of federal and regional legislation as well as directly applicable legal acts of the European Union and the European Atomic Energy Community

    a. on combating money laundering and terrorist financing, including the Money Laundering Act and Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EU) No 1781/2006 (OJ L 141, 5.6.2015, p. 1), as amended by Regulation (EU) 2019/2175 (OJ L 334, 27.12.2019, p. 1), as amended,

    b. laying down requirements for product safety and conformity,

    c. road safety requirements concerning road infrastructure safety management, safety requirements in road tunnels and admission to the occupation of road haulage operator or road passenger transport operator (bus and/or coach undertaking),

    d. requirements to ensure the safety of railway operations,

    e. maritime safety requirements concerning European Union rules on the recognition of ship inspection and survey organisations, carrier's liability and insurance in respect of the carriage of

passengers by sea, approval of marine equipment, maritime safety inspection, seafarers' training, registration of persons on board passenger ships engaged in maritime transport, and European Union rules and procedures for the safe loading and unloading of bulk carriers,

f. civil aviation safety requirements for the prevention of operational and technical safety hazards and for air traffic control,

g. requirements for the safe carriage of dangerous goods by road, rail and inland waterways,

h. with specifications for environmental protection,

i. requirements for radiation protection and nuclear safety,

j. promoting the use of energy from renewable sources and energy efficiency,

k. on food and feed safety, on organic production and labelling of organic products, on the protection of geographical indications for agricultural products and foodstuffs, including wine, aromatised wine products and spirit drinks, and traditional specialities guaranteed, on the placing on the market and use of plant protection products, and on animal health and welfare as they relate to the protection of farmed animals, the protection of animals at the time of killing, the keeping of wild animals in zoos, the protection of animals used for scientific purposes and the transport of animals and related operations,

l. on quality and safety standards for organs and substances of human origin, medicinal products for human and veterinary use, medical devices and cross-border patient care,

m. on the manufacture, presentation and sale of tobacco and related products,

n. to regulate consumer rights and consumer protection in relation to contracts between traders and consumers and to protect consumers in the field of payment accounts and financial services, price indication and unfair commercial practices,

o. the protection of privacy in electronic communications, the protection of confidentiality of communications, the protection of personal data in the electronic communications sector, the protection of the privacy of users' terminal equipment and of information stored in such terminal equipment, the protection against unreasonable harassment by means of advertising by telephone calls, automatic calling machines, facsimile machines or electronic mail, and by means of calling line identification and calling line identification suppression, and the inclusion in directories of subscribers

p. on the protection of personal data within the scope of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1; L 314, 22.11.2016, p. 72; L 127, 23.5.2018, p. 2; L 74, 4.3.2021, p. 35) in accordance with Article 2 thereof,

q. on the security of information technology within the meaning of section 2(2) of the BSI Act of digital service providers within the meaning of section 2(12) of the BSI Act,

r. to regulate the rights of shareholders of public limited companies,

s. on the audit of financial statements of public interest entities pursuant to section 316a sentence 2 of the Commercial Code,

t. on accounting, including bookkeeping, of companies that are capital market-oriented within the meaning of section 264d of the German Commercial Code, of credit institutions within the meaning of section 340(1) of the German Commercial Code, financial services institutions within the meaning of section 340(4) sentence 1 of the German Commercial Code, securities institutions within the meaning of section 340 (4a) sentence 1 of the Commercial Code, institutions within the meaning of section 340 (5) sentence 1 of the Commercial Code, insurance undertakings within the meaning of section 341 (1) of the Commercial Code and pension funds within the meaning of section 341 (4) sentence 1 of the Commercial Code,

4. infringements of federally and uniformly applicable regulations for contracting entities on the procedure for the award of public contracts and concessions and on legal protection in these procedures after the relevant EU thresholds have been reached,

5. infringements covered by section 4d (1), first sentence of the Financial Services Supervision Act (Finanzdienstleistungsaufsichtsgesetz), unless otherwise provided for in section 4(1), first sentence,

6. infringements of legal tax standards applicable to corporations and partnerships,

7. violations in the form of agreements aimed at improperly obtaining a tax advantage contrary to the objective or purpose of the tax law applicable to corporations and partnerships,

8. infringements of Articles 101 and 102 of the Treaty on the Functioning of the European Union as well as infringements of the legal provisions referred to in Section 81(2)(1), (2)(a) and (5) and (3) of the Act against Restraints of Competition,

9. infringements of provisions of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1),

10. statements made by public officials that constitute a breach of the duty to be faithful to the Constitution.

11. reporting and disclosure of information concerning

    a. infringements of the protection of the financial interests of the European Union within the meaning of Article 325 of the Treaty on the Functioning of the European Union; and

    b. infringements of internal market rules within the meaning of Article 26(2) of the Treaty on the Operation of the European Union, including European Union rules on competition and State aid going beyond item no. 8 (pls see above).

(b) Internal reports

Employers shall ensure that at least one internal reporting office is established and operated to which employees can turn (internal reporting office). The employers shall grant the internal reporting office the necessary powers to perform its duties, to check reports and take follow-up actions.

Internal reporting offices shall operate reporting channels, conduct the prescribed procedures, and take follow-up action if necessary.

Internal reporting offices shall maintain clear and easily accessible information for employees on external reporting procedures.

Internal reporting channels shall be accessible for employees and temporary workers assigned to the employer to report information on violations.

Internal reporting channels shall be designed in such a way that only the people responsible for receiving and processing the reports and the people assisting them in the performance of these tasks have access to the incoming reports.

Internal reporting channels can optionally be open to third parties who, during their professional activities, are in contact with the employer.

Internal reporting channels can also process incoming reports anonymously. However, there is no obligation for the employer to enable anonymous reports.

Internal reporting channels must allow reports to be made verbally or in text form. Verbal reporting shall be possible by telephone or other means of voice communication. At the request of the whistleblower, a face-to-face meeting with the person responsible for receiving a report from the internal reporting channel shall be made possible for a report within a reasonable time. With the consent of the person making the report, a meeting may also take place by means of video and audio transmission.

Internal reporting offices: (i) shall acknowledge receipt of a report to the person making the report after seven days at the latest; (ii) shall determine whether the reported violation falls within the material scope of breaches that can be reported; (iii) shall maintain contact with the person making the report; (iv) shall determine the validity of the report received; (v) shall request further information from the whistleblower, if necessary; (vi) shall takes appropriate follow-up action; and (vii) shall provide feedback to the person making the report within three months of acknowledging receipt of the report or, if receipt has not been acknowledged, no later than three months and seven days after receipt of the report. The feedback shall include notification of any planned follow-up action as well as any follow-up action already taken and the reasons for such action. Reporting to the person making the report may only take place to the extent that it does not affect internal enquiries or investigations and does not prejudice the rights of the people who are the subject of a report or who are named in the report.

Internal reporting offices may in particular: (i) conduct internal investigations at the employer or at the respective organisational unit and contact the persons and work units concerned; (ii) refer the whistleblower to other competent bodies; (iii) close the proceedings due to lack of evidence or for other reasons; or (iv) refer the case for further investigation to: (a) a work unit responsible for internal investigations at the employer or at the relevant organisational unit; or (b) a competent authority.

(c) External reports

The choice between an internal or an external report is essentially with the whistleblower. There is no legal obligation to file an internal report first, although this commonly will make the most sence.

External reports can be made to the competent public authorities, currently to those three listed above. These are competent for three subsets of potential reporting topics, as illustrated in detail on their websites.

Disputes concerning the decisions of an external reporting office under paragraphs 1 to 6 shall be subject to administrative appeal.

Competent public authorities:

- **Bundesamt für Justiz**, Adenauerallee 99 – 103, 53113 Bonn, Germany;
- **Bundesanstalt für Finanzdienstleistungsaufsicht**, Graurheindorfer Str. 108; 53117 Bonn, Marie-Curie-Str. 24-28, 60439 Frankfurt am Main, Germany;
- **Bundeskartellamt**, Kaiser-Friedrich-Str. 16, 53113 Bonn, Germany

Links to external channels:

- **Bundesamt für Justiz**
  https://formulare.bfj.bund.de/ffw/form/display.do?%24context=5CDC766B3DE641612E2B

- **Bundesanstalt für Finanzdienstleistungsaufsicht**
  https://www.bafin.de/DE/DieBaFin/Hinweisgeberstelle/hinweisgeberstelle_node.html

- **Bundeskartellamt**:
  https://www.bkmssystem.net/bkwebanon/report/channels?id=bkarta&language=ger

Link to Guidelines:

- https://www.bundesjustizamt.de/DE/MeldestelledesBundes/ZustaendigkeitderMeldestellen/ZustaendigkeitderMeldestellen_node.html#AnkerDokument97000

(d) Protection measures

Whistleblowers are covered by protection under German law, if: (i) they have reported internally or externally or made a disclosure in compliance with the provisions of the German Whistleblowing Act; and if (ii) the whistleblower had reasonable grounds to believe at the time of the report or disclosure that the information reported or disclosed by him/ her was true; and if (iii) the information relates to offences that fall within the scope of the German Whistleblowing Act or the whistleblower had reasonable grounds to believe that it did so at the time of the report or disclosure.

Reprisals directed against persons providing information are prohibited by law. This also applies to the threat and the attempt to exercise reprisals. If a whistleblower suffers any adverse treatment in connection with his or her professional activities and claims to have suffered such adverse treatment because of a report or disclosure under this Act, such adverse treatment shall be deemed to be reprisal for such report or disclosure.

In such a case, the person who has adversely affected the whistleblower shall prove that the adversity was based on sufficiently justified grounds or that it was not based on the report or disclosure.

Agreements that restrict the rights of persons giving notice under the German Whistleblowing Act or persons otherwise protected thereunder shall be ineffective.

Protection measures apply, mutatis mutandis, to: (i) individuals who confidentially assist the whistleblower in making an internal or external report or disclosure in a professional context, provided that the information reported or disclosed is accurate or the assisting person had reasonable grounds to believe at the time of the assistance that the information reported or disclosed by the whistleblower was accurate, and relate to offences that fall within the scope of the German Whistleblowing Act or the assisting person had reasonable grounds to believe at the time of the assistance that this was the case; (ii) third parties associated with the person providing the information who have suffered reprisals in a professional context, unless these are not based on the reporting or disclosure by the person providing the information; (iii) legal entities, partnerships with legal capacity and other associations of persons with legal capacity that are legally connected with the person providing the information as a result of a shareholding or for which the person providing the information works or with which he or she is otherwise connected in a professional context.

(e) Protection of confidentiality

All reporting offices shall maintain the confidentiality of the identity of the following individuals: (i) the whistleblower, provided that the information reported relates to offences falling within the scope of this Act or the whistleblower had reasonable grounds to believe that this was the case at the time of the report; (ii) the individuals who are the subject of a report; (iii) the other individuals named in the report.

The identity of the aforementioned individuals may only become known to the people responsible for receiving reports or for taking follow-up measures, as well as to the people assisting them in the performance of these tasks.

The requirement of confidentiality of identity shall apply regardless of whether the reporting office is responsible for the incoming report.

The identity of a whistleblower who intentionally or grossly negligently reports incorrect information on infringements shall not be protected.

The partial or full disclosure of the individuals´ identity is only possible in limited cases prescribed by the German Whistleblowing Act.

(f) Data Protection

The person responsible for receiving reports at a reporting office shall document all incoming reports in a permanently retrievable manner in compliance with the confidentiality requirements.

In the case of telephone reports or reports by means of another form of voice transmission, a permanently retrievable audio recording of the conversation or its complete and accurate transcription (verbatim record) may only be made with the consent of the person making the report.

If such consent is not given, the report shall be documented by a summary of its content (content protocol) to be prepared by the person responsible for processing the report.

If the report is made in the context of a meeting, a complete and accurate record of the meeting may be made and kept with the consent of the person making the report.

The recording may be made by creating an audio recording of the conversation in a permanently retrievable form or by a verbatim record of the meeting created by the person responsible for processing the report.

The person making the report shall be given the opportunity to review the transcript, correct it if necessary and confirm it by his or her signature or in electronic form.

If an audio recording is used to prepare minutes, it shall be deleted as soon as the minutes have been completed.

The documentation shall be deleted three years after the conclusion of the proceedings.

The documentation may be kept longer to meet requirements under this Act or other legislation for as long as is necessary and proportionate.

The processing of personal data Law by internal and external offices is permissible under the German Whistleblower Act insofar as this is necessary for the fulfilment of their tasks. Particularly sensitive personal data within the meaning of Art. 9 (1) GDPR are also included. Information from which conclusions can be drawn about the person of the whistleblower must be kept secret.

(g) Protection from retaliation

In the event of a violation of the prohibition of reprisals, the perpetrator shall be obliged to compensate the person making the reference for any resulting damage.

A violation of the prohibition of reprisals shall not give rise to a claim for the establishment of an employment relationship, a vocational training relationship or any other contractual relationship or for career advancement.

(h) Limitation of liability for Reporting persons

A whistleblower shall not be held legally responsible for obtaining or accessing information that (s)he has reported or disclosed unless the obtaining as such or the access as such constitutes an offence in its own right.

A whistleblower does not breach any restriction on disclosure and cannot be held legally responsible for the disclosure of information made in a report or disclosure, provided that the whistleblower had reasonable grounds to believe that the disclosure of the information was necessary to detect an infringement.

(i) Sanctions

Anyone who knowingly discloses incorrect information in contravention of the German Whistleblowing Act shall be guilty of an administrative offence.

A person commits an administrative offence if he/ she: (i) obstructs a notification or communication; (ii) fails to ensure that an internal reporting office is established and operated, or (iii) contrary to the provisions of the German Whistleblowing Act takes a reprisal.

It is also an administrative offence to fail intentionally or recklessly to maintain confidentiality in contravention the provisions of the German Whistleblowing Act. Anyone who negligently commits such shall be guilty of an administrative offence.

An attempt to commit an administrative offence may be punished in the cases referred to above in numbers 1 and 3.

An administrative offence may be sanctioned with a fine of up to 10.000,-- EUR, 20.000, or up to EUR 50.000,-- EUR, depending on the offence committed.

5.4 Poland

Poland legislation is not yet complete in 2023. The detailed requirements will be updated at a later date.

5.5 Portugal

(a) Breaches that can be reported in Portugal

It is possible to report breaches concerning:

- The act or omission contrary to the rules of the internal market referred to in paragraph 2 of article 26 of the TFUE, including the rules of competition and state aid, as well as the rules of corporate taxation;
- Violent crime, especially violent and highly organized crime, as well as the crimes predicted in paragraph 1 of article 1 of Law no. 5/2002, of 11 January, which establishes measures to combat organized and economic and financial crime;
- The act or omission that goes against the purpose of the rules or regulations covered by provisions a) to c);
- In the domains of homeland security, for the purposes of this law, an act or omission contrary to the contracting rules contained in the acts of the Federal Government is considered an infraction Europeans referred to in Part I.A of the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council, or which is contrary to the purposes of these rules.

(b) Internal reporting channel and form and admissibility of complaints

The internal whistleblowing channels allow for the safe submission and follow-up of complaints, in order to guarantee the completeness, integrity and conservation of the complaint, the confidentiality of the identity or

anonymity of the whistleblowers and the confidentiality of the identity of third parties mentioned in the complaint, and to prevent access by unauthorized personal.

The internal reporting channels are operated internally, for the purpose of receiving and following up on reports, by persons or services designated for this purpose, without prejudice to the following paragraph.

The reporting channels may be operated externally, for the purpose of receiving complaints.

For following up complaints, the reporting channels must be operated internally.

Independence, impartiality, confidentiality, data protection, secrecy, and absence of conflicts of interest must be guaranteed in the performance of duties.

The internal whistleblowing channels allow, namely, the presentation of complaints, in writing and or verbally, by workers, anonymously or with the whistleblower identified.

If a verbal complaint is admissible, the internal complaint channels allow for its presentation by telephone or through other voice message systems and, at the request of the complainant, in a face-to-face meeting.

The complaint may be submitted using means of electronic authentication with a citizen's card or digital mobile key or using other means of electronic identification issued in other Member States and recognized for this purpose under the terms of article 6. of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014, provided that, in any case, the available means are available.

(c) External reports

Competent public authority: MENAC - Mecanismo Nacional Anticorrupção.

Link to external channel: https://mec-anticorrupcao.pt/.

Link to Guidelines: https://mec-anticorrupcao.pt/.

See Lei n. 93/2021 de 20 de dezembro.

External complaints are submitted to authorities that, according to their attributions and competences, should or may know about the matter in question in the complaint, including: The Public Ministry; Criminal police bodies; The Bank of Portugal; Independent administrative authorities; Public institutes; General inspections and equivalent entities and other central services of the direct administration of the State endowed with administrative autonomy; Local authorities and Public associations.

(d) Protection measures

Whistleblowers are entitled, in general terms, to legal protection and may benefit, in general terms, from witness protection measures in criminal proceedings.

The competent authorities provide the necessary assistance and collaboration to other authorities for the purpose of guaranteeing the whistleblower's protection against acts of retaliation, including by certifying that the whistleblower is recognized as such under this law, whenever this is so request.

The Directorate-General for Justice Policy provides information on the protection of whistleblowers on the Justice Portal, without prejudice to the mechanisms for access to law and courts.

(e) Sanctions

Law No. 93/2021 of December 20 provide for administrative sanctions applied by MENAC: (i) Very serious offenses with fines from €1 000 to €25 000 when the agent is an individual and from €10.000 to €250.000

when the agent is a legal person; (ii) Serious offenses with fines from €500.00 to €12.500 if the agent is an individual and from €1.000 to €125.000 if the agent is a legal person.

5.6 Romania

(a) Breaches that can be reported

In Romania, the breach of any law can be reported, not only in the fields stipulated in paragraph 2.2, if the breaches represent disciplinary violations, misdemeanors, or crimes or if they contravene the object/purpose of a law.

(b) Internal reports

In Romania, under the applicable law, Companies with more than 249 employees cannot share the reporting channel and its handling with other Companies. Therefore, such Companies shall provide for a local reporting channel, other and additional than the Group channel. For companies based in Romania with more than 249 employees, a local channel is provided, additional to the Group one. The local channel is handled by a nominated local Whistleblowing Officer or Committee.

(c) External reports

Competent public authority: the National Integrity Agency.

Link to external channel: https://www.integritate.eu/Home.aspx.

Link to Guidelines: https://avertizori.integritate.eu/.

External reports may be addressed to (i) the authorities and public institutions that, according to the special legal provisions, receive and resolve reports regarding violations of the law, in their field of competence; (ii) The National Integrity Agency or (iii) other public authorities and institutions to which the National Integrity Agency submits the reports for competent resolution.

The Reporting person can choose between the internal and external reporting channel, having into consideration aspects such as: (i) the risk of retaliations in case of internal reports; (ii) the impossibility of remedying the breach effectively through internal reports.

(d) Protection measures

At the request of the Reporting person under disciplinary investigation, within a maximum of one year from the date of the report, the Bar provides him/her free legal assistance during the disciplinary procedure.

At the request of the Reporting person who challenges the retaliation measures in a Court of law, the Bar ensures him/her free legal assistance.

At the request of the Reporting person who is subject to disciplinary investigation because of internal, external reporting or public disclosure, the disciplinary commission has the obligation to invite the press and a representative of the trade union or professional association or a representative of the employees, as the case may be. The announcement is made on the Company website, at least 3 working days before the meeting. If this obligation is not fulfilled, the disciplinary report and the disciplinary sanction are null and void.

(e) Limitation of liability for Reporting persons

In legal proceedings regarding at infringements such as infringement of the right to image, infringement of copyright, infringement of professional secrecy, infringement of data protection rules, disclosure of trade secrets or actions for compensation, the Reporting persons cannot be held liable.

Reporting persons have the right to invoke said reporting to pursue the closure of the case, provided they had reasonable grounds to believe that the reporting was necessary to disclose a violation of the law.

If a person reports information regarding violations of the law and such information includes trade secrets, such reporting or public disclosure is considered lawful.

(f) Protection of confidentiality

The identity of the Reporting person, of the Person involved, or of the individuals mentioned in the report can be disclosed only if this is an obligation imposed by law, in compliance with the conditions and limits provided by it. In this case, the persons are previously informed, in writing, about the disclosure of their identity and the reasons for the disclosure of the confidential data in question. The obligation does not exist if the information would jeopardize investigations or legal proceedings.

(g) Sanctions

Administrative sanctions applied by the National Integrity Agency:

- preventing, by any means, the reporting by the person designated to receive and record the reports or by the person who is part of the department designated for this purpose - fine from 2.000 RON to 20.000 RON;
- unjustified refusal of companies to respond to the requests of the Agency or other authorities - fine from 3.000 RON to 30.000 RON;
- failure to comply with the obligation to establish internal reporting channels - fine from 3.000 RON to 30.000 RON;
- non-compliance by legal entities with the obligation to design, establish and manage the method of receiving reports in such a way as to protect the confidentiality of the identity of the reporting person and of any third party mentioned in the report and to prevent unauthorized personnel from accessing the report - fine from 4.000 RON to 40.000 RON;
- violation by natural persons of the obligation to maintain confidentiality regarding the identity of the reporting person, of the person concerned or of third parties - fine from 4.000 RON to 40.000 RON.
- reporting information regarding violations of the law, knowing that they are untrue - fine from 2.500 RON to 30.000 RON.

5.7 Slovakia

Competent public authority: ÚOO – Úrad na ochranu oznamovateľov (Whistleblower protection office).

Link to external channel: www.oznamovatelia.sk.

Link to Guidelines: www.oznamovatelia.sk.

SECTION 3

1. SPECIFIC PURPOSE OF GDPR APPLICATION IN BRAZIL

The requirements for data protection in Brasil are set out in the law 13.709/2018 - General Data Protection Law (**LGPD**), which came into force in the country in August 2020. Inspection is the responsibility of the National Data Protection Authority (ANPD), a body subordinate to the Presidency of the Republic, responsible for overseeing compliance with the law, preparing guidelines, and applying sanctions in cases of irregularity. Other bodies may be related to the enforcement of the law when appropriate, such as the Public Ministry, to deal with the issue of diffuse rights of citizens and others.

Link to external channel: https://super.presidencia.gov.br/controlador_externo.php?acao=usuario_externo_logar&acao_origem=usuario_externo_gerar_senha&id_orgao_acesso_externo=0

The submission of requests to the ANPD (Complaints and Petitions) must be carried out by filling out a form and must be sent through the Electronic Petition of SUPER.BR (Single System of Electronic Process in Network). In the SUPER system, select the type of process "ANPD – Complaint" or "ANPD – Holder Petition", depending on your demand. Attach the completed form to the process, preferably in PDF format, and additional documents, if any. Applications submitted using the forms below can be followed up on the ANPD electronic process platform and must be identified. Forms without identification will not be received. Petitions by holders cannot be sent anonymously. If you want to make an anonymous report, they should only be sent through the Fala.br Platform. It is not possible to follow up on the case if it is submitted as an anonymous report.

Link to Guidelines: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia peticao-de-titular.

2. PECULIARITIES - GUIDELINES OF THE BRAZILIAN GOVERNMENT

When submitting a complaint or owner petition form to the ANPD, please be aware that the content of your request, including your personal information and attached documents, may be shared with the person in charge or the legal representative of the treatment agent about which you are submitting the complaint or request.

Before submitting your complaint or owner petition, it is important to know some information:

- Holder petition is a request made to the ANPD by the holder of personal data when he is unable to exercise his rights before the controller of personal data. You can exercise your rights in a specific situation, where a company or a public body, for example, collects, stores, uses or shares your personal data. The exercise of rights must first be requested directly from the controller responsible for the personal data. And, if your request has not been met or the response given by the controller has not been satisfactory, you can notify the ANPD through a 'Petition of Holder'. It is important to emphasize, however, that the rights of the holder are not absolute and cannot always be met by the controller, as in the case of the request for deletion of data in which the controller has a legal obligation to keep this data, for example.

- When submitting your application to the ANPD, you must present documents or information that proves your attempt to exercise your right before the controller. Therefore, anonymous petitions from holders will not be accepted by the ANPD.

- When trying to exercise their rights through the official channels of the personal data controller, it is recommended that the data subject keep the controller's contact information, such as, for example, service protocol number, instructions received, messages and emails. Contact information for the person in charge of processing personal data is generally available on the privacy policy pages of the controllers on their websites. When sending your petition to the ANPD, be aware that it will be analyzed

in aggregate, that is, your petition will not necessarily be analyzed individually. The LGPD provides a series of rights to the holder of personal data in relation to the processing of their data.

These rights include:

- The right to confirm the existence of processing of personal data by the controller,
- The right to access your personal data,
- The right to request correction of information that is incomplete or out of date,
- The right to request the revocation of the consent given to the controller of the personal data,
- The right to request information about the sharing of your personal data and, in some situations, the right to request the deletion of your data.

Complaints are communications made to the ANPD by any person, natural or legal, of an alleged violation of Brazilian personal data protection legislation, other than the holder's petition.

Complaints of non-compliance with the LGPD have the characteristic of not necessarily relating to a specific situation of a particular holder of personal data. Generally, these are situations that affect a group of data subjects or that make it impossible for data subjects to exercise their rights.

Examples of situations that can be reported are:

- the discriminatory treatment of personal data,
- the excessive collection of personal data,
- the absence of a person in charge of processing personal data,
- the non-existence of a communication channel for the exercise of rights,
- the absence of adequate security measures,
- the absence of a privacy policy, among others.

Without the identification of the treatment agent, it is not possible for the ANPD to act, as, for example, in the case of contacts or calls that hang up without saying anything, right after the service; or in the case of spam emails that do not identify the sender.

It is important to highlight those cases of crimes involving personal data, such as, for example, fraud with the purpose of harming data subjects or obtaining undue resources or advantages with the use of their personal data, must be reported to the competent police authorities.

The ANPD, in accordance with its legal attributions, does not specifically investigate crimes, but administrative infractions, and may apply the sanctions provided for in the LGPD to offenders, such as warnings, fines, blocking, among others.

Complaints not related to the LGPD or made in a general way will not be accepted. The situation presented to the ANPD must be: (i) clearly written; (ii) relating to a specific situation involving personal data; (iii) related to non-compliance with personal data protection legislation (General Data Protection Law).

All requests received, as well as the assessment of controller responses by the holders, when applicable, will be considered in the planning of our inspection actions, regulatory improvements and educational actions proposed by the ANPD.

The requirements, as a rule, will be analyzed in aggregate and any measures resulting from them will be adopted in a standardized way. In this way, the ANPD will not intervene directly in your concrete and specific situation related to the processing of your personal data or the exercise of your rights, but your situation will be considered in broader plans and actions that can reach, directly or indirectly, a set of holders with situations equivalent or like yours.

In general, the ANPD will not send you an individual response and will not give you an individual opinion on your application.

However, requests referring to serious situations that may affect many people may, exceptionally, be handled individually.

This procedure is regulated by the LGPD and by articles 20, 25 and 26 of the Regulation of the Inspection Process and Sanctioning Administrative Process, approved by Resolution CD/ANPD No. 1/2021.

ANPD does not issue any type of certificate for professionals to act as Person in Charge of Personal Data Processing.

It is also important to clarify that there is no legal requirement for registration, before the ANPD or before private associations, of data protection professionals or supervisors, as a condition for exercising the profession or as a requirement for hiring them.

ANPD does not officially recognize any registration mechanisms in private companies for these professionals.