WHISTLEBLOWER POLICY CLAES RETAIL GROUP NV

The law of November 28, 2022 on the protection of whistleblowers of breaches of Union or national law established within a legal entity in the private sector, is a transposition of the European Whistleblower Directive 2019/1937. The law provides protection to employees and third parties who wish to report information about a violation of Union law within a legal entity in the private sector.

This Whistleblower Policy aims to provide transparency to employees of the CLAES RETAIL GROUP NV[1], as well as certain other interested third parties, about the channels in place to report such (alleged) irregularities within C.R.G..

In this way, C.R.G. wishes to act against any illegal, deceptive or other not permitted practices or acts that fall under the control of the company or any of its subsidiaries, to ensure an independent and confidential investigation and to avoid possible conflicts of interest. However, this policy does not imply a reporting obligation, but an opportunity for C.R.G. employees and third parties to report, with the application of certain safeguards, any possible irregularities within the company.

1. Definitions

For the purposes of this policy, the following definitions shall apply:

- **"information about breaches"**: information, including reasonable suspicions, about actual or possible breaches, which have occurred or are highly likely to occur, as well as attempts to conceal such breaches;

- **"reporting"** or **"to report"**: the oral, written or electronic communication of information about breaches;

- **"internal reporting"**: the oral or written communication of information about breaches within a legal entity in the private sector;

- **"external reporting"**: communication, orally or in writing, to the federal coordinator or to competent authorities of information about violations;

- **"disclosure"** or **"to disclose":** making information about breaches publicly available;

- **"reporter"** or **"whistleblower"**: a person who reports or discloses information about breaches;

- **"work-related context"**: current or former professional activities in the private sector that make possible that, regardless of the nature of those activities, persons obtain information about violations and in which those persons may face retaliation if they were to report such information;

- **"facilitator"**: a natural person who assists a reporter in the reporting process and whose assistance must be confidential;

[1] CLAES RETAIL GROUP NV, is the holding company above the fashion brands JBC, CKS and Mayerline. This policy applies to following legal entities:
- C.R.G. NV, with registered office located at Centrum Zuid 3401, 3530 Houthalen, KBO 0462.417.806
- JBC NV, with registered office located at Centrum Zuid 3401, 3530 Houthalen, KBO 0429.340.608
- Mayerline NV, with registered office located at Centrum Zuid 3401, 3530 Houthalen, KBO 0400.573.277.

- **"party concerned"**: a natural or legal person mentioned in the report or in the disclosure as the person to whom the breach is attributed or with whom that person is associated;

- **"reprisal"**: any direct or indirect action or omission in response to an internal or external report or disclosure, which leads to or may lead to unjustified detriment to the reporter.

2. Scope of Personnel:

This policy applies to reporters who have received information about breaches in a work-related context. This means that the reporting channels and protection mechanisms mentioned below are open to, among others:

1. Current employees of C.R.G.;
2. Former employees in case information about breaches was obtained in the context of a terminated work relationship;
3. Candidate employees in case information about breaches was obtained during the recruitment process or other pre-contractual negotiations;
4. Independent service providers within C.R.G. (such as freelancers, consultants);
5. Shareholders and individuals belonging to the administrative, managerial, or supervisory body of C.R.G., including members not involved in daily management, volunteers, and paid or unpaid interns;
6. Anyone working under the supervision and direction of contractors, subcontractors, and suppliers;
7. Facilitators;
8. Third parties connected to the reporters who may become victims of reprisals in a work-related context, such as colleagues or family members of the reporters;
9. Legal entities owned by the reporters, for which the reporters work or with which the reporters are otherwise connected in a work-related context.

3. Material Scope:

The reporting channels can be used to report the following breaches:

1° Breaches related to the following areas:

a) public procurement;

b) financial services, products and markets, prevention of money laundering and terrorist financing;

c) product safety and product compliance;

d) transport safety;

e) environmental protection;

f) radiation protection and nuclear safety;

g) food and feed safety, animal health, and animal welfare;

h) public health;

i) consumer protection;

j) protection of privacy and personal data, and security of network and information systems;

k) combating tax fraud;

l) combating social fraud.

2° Breaches (such as fraud) harming the financial interests of the European Union (cf. Article 325 of the Treaty on the Functioning of the European Union);

3° Breaches of Union rules on competition and state aid, and other breaches related to the internal market (cf. Article 26, paragraph 2, of the Treaty on the Functioning of the European Union).

4° Attempts to conceal information related to any of the above matters.

Excluded from the application of this whistleblowers policy, however, are:

- Complaints related to violence, bullying, and unwanted sexual behavior, which an employee who believes to be a victim of such actions can report to the designated confidential contact person specified in the employment regulations or to the psychosocial prevention advisor of the external service for prevention and protection at work.
- Reports concerning classified information;
- Reports based on information covered by medical professional secrecy;
- Reports based on information covered by the confidentiality of judicial deliberations.
- Complaints related to the services provided by C.R.G. (such as complaints regarding invoice payment).

When making a report, a whistleblower must always act in good faith. The report must be based on reasonable grounds. If the report contains false, unfounded, or opportunistic allegations, or is made with an incorrect motive, such as to defame or cause harm to others, C.R.G. may disregard the report and, if necessary, take appropriate measures.

4.Reporting Procedures

There are three ways to report:

- Internal reporting
- External reporting
- Disclosure

If you have identified a (potential) breach, become aware of it, or reasonably suspect that it has occurred or is occurring within C.R.G., you are advised to initially report it internally.

4.1. Internal Reporting Procedure

A reporter, as described under the 'Scope of Personnel', who believes there is an irregularity, as described in the 'Scope of Material', can make a report to the designated complaints handler. A report is preferably made by email or in writing, but can also be made orally, preferably by appointment, over the phone or, at the request of the reporter, through a physical meeting within a reasonable timeframe. The designated complaints handler for C.R.G. is:

Annick Thijs

Centrum Zuid 3401

3530 Houthalen

E.: blowthewhistle@claesretailgroup.com (+32 11 60 84 00)

The complaints handler receiving a report sends a confirmation of receipt to the reporter within 7 working days after receipt.

The complaints handler records the report with the date of receipt and is the only one who knows the identity of the reporter. The confidentiality of the identity of the reporter and any third parties mentioned in the report is always guaranteed. Unauthorized staff members do not have access to the internal reporting channel. If there are uncertainties in the initial report, the complaints handler will request clarification.

The complaints handler is responsible for careful follow-up of each report (see Incident Response Plan):

Incident Response Plan

1. Upon receiving the report, the complaints handler convenes an internal committee. The internal committee is composed of the management members of the following departments: legal - IT - HR - finance. If the report concerns potential breaches within one of the departments of the internal committee, the relevant department will be excluded from the initial discussion of the report. The complaints handler will confidentially and anonymously inform the internal committee about the report.
2. The internal committee determines the necessary investigative measures regarding the alleged irregularities, such as, for example, but not limited to:

   • Interviewing the reporter by the complaints handler about the alleged irregularities.

   • Interviewing the person or persons who were reported to be involved in the alleged irregularities.

   • Gathering information and consulting sources necessary to verify the alleged irregularities signaled by the reporter.
3. The internal committee examines the potential impact of the report on the company's operations, reputation, etc.
4. The internal committee orally and in writing reports its findings to the executive board (the "management") of C.R.G..
5. The executive board of C.R.G. makes a decision and takes any measures based on the report of the complaints handler. If the report concerns a member of the executive board, the report is addressed to the delegated directors of C.R.G..
6. The reporter and any accused individuals are informed of the conclusion of the investigation.

Protection

1. The handling of a report is carried out with adherence to confidentiality.
2. The executive board of C.R.G. declares that a report made by an employee to the complaints handler under this whistleblower regulation may not negatively affect the functioning or career opportunities of that employee within the company.
3. The reporter is asked to commit to treating their report confidentially and not to disclose it directly or through third parties until the executive board of C.R.G., via the complaints handler, has communicated the conclusion of the investigation.
4. A reporter who intentionally made a manifestly unfounded report, and thus unlawfully used the reporting procedure of this whistleblower regulation, may be sanctioned for this (see further).

Registration of Reports

C.R.G. keeps a record of each received report in accordance with the aforementioned confidentiality requirements. Reports are kept for the duration of the contractual relationship.

If a telephone line without call recording or another voice messaging system without call recording is used for the report, the company reserves the right to register the oral report in the form of an accurate report of the conversation, prepared by the staff member responsible for handling the report. The reporter always has the opportunity to review, correct, and sign the report of the conversation.

If a person requests a meeting with the complaints handler to make an internal report, C.R.G. ensures, with the consent of the reporter, that a complete and accurate record of the meeting is kept in a durable and retrievable form. C.R.G. reserves the right to register the oral report in the following ways:

- by making a recording of the conversation in a durable and retrievable form; or
- by an accurate report of the meeting, prepared by the staff member responsible for handling the report. The reporter always has the opportunity to review, correct, and sign the written representation of the meeting report.

Right to Protection of Privacy

The personal data of the reporter and the accused person or persons are processed in a confidential manner and solely for the purpose of handling a report and the subsequent investigation in accordance with the privacy notice. The individuals concerned may invoke the right of access and rectification of the data processed concerning them in accordance with the General Data Protection Regulation 2016/679 and the privacy notice. They may also address the Data Protection Authority for this purpose. They do not have access to third-party data.

Privacy Statement for Internal Reports

By using the internal reporting channels provided in this Whistleblower Policy, you consent to the processing of your personal data for the purposes outlined in this Whistleblower Policy.

a) Processing of Personal Data

C.R.G. will process personal data of (1) the complainant and (2) the involved individual (i.e., accused person) in the context of its "Whistleblower Policy" as the data controller.

Specifically, C.R.G. will process the following personal data related to the complaint of the complainant:

- identification and contact details of the complainant (name/first name/email/phone number) and any other involved parties;

- (possible) recording of the report;
- the relationship of the complainant to C.R.G.;
- the content of the complaint; and
- the (personal) data associated with the complaint (including the accused person and evidence).

C.R.G. does not process special categories[2] of personal data of the complainant, unless strictly necessary in the context of complaint handling. If special categories of personal data are collected by C.R.G. in the context of the "Whistleblower Policy," these personal data will be processed with the necessary security and in accordance with the appropriate legal basis.

C.R.G. always processes the above-mentioned personal data in compliance with the applicable European and national privacy laws, including but not limited to (1) the General Data Protection Regulation (EU) 2016/679 (hereinafter "GDPR") and (2) the law of July 30, 2018, regarding the protection of natural persons with regard to the processing of personal data.

b) Purposes of processing

Furthermore, C.R.G. processes the above-mentioned personal data in a confidential manner and solely for the purpose of implementing the "Whistleblower Policy" resulting from compliance with legal obligations. For questions regarding the processing of your personal data, you can contact us via e-mail at legal@jbc.be.

Specifically, C.R.G. processes this personal data to comply with the purposes arising from the above-mentioned legislation and its "Whistleblower Policy," in order to address, assess, and, if necessary, further investigate the complainant's report, as well as potentially defend itself in the context of any legal proceedings (i.e. personal data is processed based on Article 6.1 (c) and (f) of the GDPR "necessary for compliance with a legal obligation" and "legitimate interest").

c) Transfer

The personal data collected in the implementation of this Whistleblower Policy may be shared with specifically designated (managerial) employees of C.R.G. and with independent service providers who represent the interests of C.R.G., if necessary to further follow up on the report. Section 4.1 of this Whistleblower Policy sets out which employee has access to the personal data, when, and for what reason.

If we are legally obligated to do so, your personal data may be disclosed to supervisory authorities, tax authorities, and law enforcement agencies.

d) Security

C.R.G. has implemented appropriate technical and organizational measures to protect the received personal data and to ensure the purposes of the "Whistleblower Policy." Specifically, C.R.G. has implemented security standards that safeguard the personal data against loss, misuse, alteration, and unauthorized access.

e) Retention Period

[2] Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a person's sex life or sexual orientation.

The personal data will be retained for as long as necessary for the processing and handling of the report, including any measures and follow-up thereof. The data may be retained longer if and to the extent necessary in the context of legal proceedings.

f) Rights

Under certain conditions, the complainant has the right to:

- access their personal data;
- correct their personal data;
- delete their personal data;
- restrict the processing of their personal data;
- object to the processing of their personal data;
- exercise the right to data portability;
- request the transfer of their personal data;
- withdraw their consent at any time (if applicable).

The complainant can exercise the above rights by contacting legal@jbc.be and providing the necessary supporting documents to C.R.G. Please note that as a result of exercising certain of the above rights, C.R.G. may not be able to comply with its obligations under the "Whistleblower Policy" and/or applicable legislation, and will inform the complainant that the exercise of the above rights may not be possible given the current applicable regulations. C.R.G. will make all reasonable and practical efforts to comply with the request provided that it is in accordance with applicable law and professional standards.

g) Complaints

The complainant has the option to file a complaint with the Belgian Data Protection Authority if they believe that the processing of their personal data is in violation of the GDPR (https://www.gegevensbeschermingsautoriteit.be/contact). The complainant also has the option to contact C.R.G. via privacy@jbc.be.

4.2. **External reporting procedure**

A reporter has the option of reporting information about violations by using the external reporting channels and procedures after first making a report through internal reporting channels or by reporting immediately through the competent authorities.

It is highly recommended to report (suspected) breaches internally first. Internal reports remain the most effective in enabling C.R.G. to thoroughly investigate the matter and take appropriate measures to address the misconduct.

Competent authorities

The authorities competent to receive reports, provide feedback and offer follow-up on notifications are the following:

1. the Federal Public Service Economy, K.M.O., Middle Classes and Energy;

2. the Federal Public Service Finance;

3. the Federal Public Service Health, Food Chain Safety and Environment;

4. the Federal Public Service of Mobility and Transport;

5. the Federal Public Service Employment, Labor and Social Dialogue;

6. the Programming Public Service Social Integration, Poverty Reduction, Social Economy and Metropolitan Policy;

7. the Federal Agency for Nuclear Control;

8. the Federal Agency for Medicines and Health Products;

9. the Federal Agency for the Safety of the Food Chain;

10. the Belgian Competition Authority;

11. the Data Protection Authority;

12. the Financial Services and Markets Authority;

13. the National Bank of Belgium;

14. the College of Supervision of Auditors;

15. the authorities reported in article 85 of the law of September 18, 2017 on the prevention of money laundering and terrorist financing and restricting the use of cash;

16. the National Committee for the Security of Drinking Water Supply and Distribution;

17. the Belgian Institute of Postal Services and Telecommunications;

18. the National Institute for Health and Disability Insurance;

19. the National Institute for the Social Insurance of the Self-Employed;

20. the National Employment Service;

21. the State Social Security Administration;

22. the Social Intelligence and Investigation Service;

23. the Autonomous Anti-Fraud Coordination Service (CAF);

24. the Shipping Inspectorate.

In the absence of designation or if no authority considers itself competent to receive a report, then the Federal Ombudsman shall act as the competent authority to receive reports, provide feedback and providing follow-up on reports.

Procedure for external reports

A whistleblower who believes that a violation has occurred may make a report to the competent authority or to the Federal Ombudsman.

Each authority must have established an independent and autonomous external reporting channel for receiving and handling information about breaches. The external reporting channels offer the possibility

of written and oral reporting. Oral reporting is possible via telephone or other voice messaging systems and, at the whistleblower's request, through a physical meeting within a reasonable period of time.

The appointed competent authorities determine, through regulations or a circular, concrete rules of procedure for receiving and processing reports.

The competent authority shall always send an acknowledgement of that receipt, unless specifically requested otherwise by the whistleblower or unless the competent authority considers on reasonable grounds that an acknowledgement of receipt of the report would not protect the identity of the whistleblower.

The competent authority shall carefully follow up on reports, including anonymous reports, and provide the whistleblower within a reasonable period not exceeding three months or, in duly justified cases, six months, feedback, except where a provision of law prevents it.

The competent authority shall inform the whistleblower of the final outcome of the investigations following the report, subject to the national provisions applicable to it.

Any authority that has received a report, but is not competent to deal with the reported violation, shall, within a reasonable time and in a secure manner, transmit the notification to the Federal Coordinator, who shall in turn transmits it to the competent authority, and promptly informs the whistleblower of this transmission.

If the authority that received the report is aware that other authorities are also competent, the report shall be transmitted within a reasonable time and in a secure manner to the federal coordinator, who shall transmit it to the competent authorities and ensure its coordination.

External reporting channels must always meet the requirements of independence and autonomy. This means that they meet each of the following criteria:

1. by their design, set-up and management, the channels ensure the completeness, integrity and confidentiality of information and are not accessible to unauthorized personnel of the competent authority;

2. they provide the possibility, for the purpose of further investigations to be carried out, to permanently storage.

Competent authorities are required by law to publish on a separate, easily identifiable and accessible page of their website to publish all necessary information, such as:

1° the conditions of eligibility for protection;

2° the necessary contact details for external reporting channels, in particular electronic and postal addresses, and the telephone numbers for such channels, indicating whether telephone calls are recorded;

3° the procedures applicable to the reporting of Breaches,

4° the confidentiality and privacy rules;

5° the manner of follow-up to be provided to reports;

6° the remedies and procedures for protection against retaliation and the availability of confidential advice, for persons considering reporting;

7° a statement clearly explaining the conditions under which persons reporting to the competent authority are protected from incurring liability for a breach of the confidentiality rule; and

8° the contact information of the federal coordinator and of the Federal Institute for the Protection and promotion of human rights.

4.3. **Disclosure**

In addition to the possibility of making a report through the internal reporting channel or the external reporting channels, any person has the option to disclose the information related to a breach.

A reporter who makes a disclosure is eligible for the protections listed below under this policy if:

1. the employee first made an internal and external disclosure, or immediately made an external disclosure, but no appropriate action was taken in response to that report within the specified time frames;

or

2. the employee has reasonable grounds to believe that:

a. the breach may pose an imminent or real danger to the public interest; or

b. there is a risk of retaliation in the event of external reporting, or it is unlikely that the breach will be effectively remedied, due to the particular circumstances of the case, because for example, evidence may be withheld or destroyed, or an authority may collude with the perpetrator of the breach or is involved in the breach.

5. Protective measures

Protection Conditions

A reporter is eligible for protection provided he/she:

- had reasonable cause to believe that the reported information about violations at the time of the report was accurate and that that information was within the scope of this policy. This criterion shall be assessed against a person who is in a comparable situation and has comparable knowledge; and

- they reported information internally or externally, or disclosed information in accordance with this Whistleblower Policy.

The whistleblower will not lose the benefit of the protection on the sole ground that the report made in good faith is found to be incorrect or unfounded.

Facilitators and third parties associated with the reporters are also eligible for the protections set forth below if they had reasonable cause to believe that the reporter fell within the scope for protection of this policy.

Protective measures against retaliation

If the reporter, facilitator or third party associated with the reporter meets the above conditions, he shall enjoy protection against any form of retaliation, including threats and attempts of retaliation. Retaliation includes the following measures:

1. suspension, temporary retirement, dismissal or similar action;

2. demotion or refusal of promotion;

3. transfer of duties, change of job location, reduction in pay, change of working hours;

4. withholding of training;

5. negative performance evaluation or work reference;

6. imposition or application of a disciplinary action, reprimand or other sanction, such as

a financial penalty;

7. coercion, intimidation, harassment or exclusion;

8. discrimination, adverse or unequal treatment;

9. failure to convert a temporary employment contract into an employment contract of indefinite duration period, in the event the employee had the legitimate expectation that he would be offered employment for an indefinite term would be offered;

10. non-renewal or early termination of a temporary employment contract;

11. damages, including loss of reputation, especially on social media, or financial loss, including loss of sales and revenue;

12. blacklisting based on an informal or formal agreement for an entire sector or industry, preventing the person from finding employment in the sector or industry;

13. early termination or cancellation of a contract for the provision of goods or services;

14. revocation of a license or permit;

15. psychiatric or medical referrals.

No civil, criminal or disciplinary action may be brought against any person who reports information about violations or makes a disclosure pursuant to this policy, no civil, criminal or disciplinary actions may be brought, nor professional sanctions may be imposed because of such reporting or disclosure.

Reporters cannot be held liable for acquiring or accessing the information reported or disclosed unless such acquisition or access in and of itself constituted a criminal offense.

Any protected person who believes he or she has been victimized or threatened with retaliation may file a reasoned complaint with the Federal Coordinator, who will initiate an extrajudicial protection procedure in accordance with art. 26 et seq. of the law of November 28, 2022 on the protection of reporters of violations of Union or national law established within a legal entity in the private sector.

Without prejudice to any other administrative or extrajudicial remedy, any protected person has the right to file an appeal before the Labor Court in case of reprisals in accordance with Article 578 of the Judicial Code.

Support measures

Each protected person has access to the following support measures.

1. Complete and independent information and advice, easily accessible and free of charge are available, on the remedies and procedures that protect against retaliation as well as on the rights of the data subject, including their rights regarding protection of personal data; in addition, the reporter must be informed that he or she is eligible for the protection measures provided for in this law; technical advice regarding any authority involved in the protection of the reporter;

2. Legal assistance in cross-border criminal and civil proceedings in accordance with Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in proceedings for the execution of a European Arrest Warrant and Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters and legal aid 15/24 in other proceedings as well as legal advice or other legal assistance, in accordance with the provisions on second-level legal assistance and legal aid;

3. Support measures, including technical, psychological, media-related and

4. Social support, for the reporters referred to in Article 6;

5. Financial assistance to reporters in legal proceedings.

Any Protected Person can also always contact the Federal Institute for the Protection and Promotion of Human Rights for legal, psychological, social, IT and communication support. The Federal Institute is also the central information point regarding the protection of whistleblowers.

Contact details:

Federal Institute for the Protection and Promotion of Human Rights Rue de Louvain 48, 1000 Brussels, e-mail address: info@firm-ifdh.be, for more

information: https://federaalinstituutmensenrechten.be/nl.

6. Sanctions for violation of the Whistleblower Policy.

Any employee who violates the rules of this Whistleblower Policy may be sanctioned with one of the sanctions determined by the labor regulations. The employee who intentionally makes a manifestly unfounded report, thus unlawfully using the reporting procedure of this Whistleblower Policy, may also be sanctioned with one of the sanctions determined by the Labor Code.

Persons associated with C.R.G. who do not have the status of employees of the company, who have violated the rules set forth in this Whistleblower Policy may be sanctioned by C.R.G. with a disciplinary sanction.

Whistleblowers may be punished in accordance with Articles 443 to 450 of the Criminal Code when they are found to have intentionally reported or disclosed false information. Persons who suffer damages as a result of such reports or disclosures are entitled to compensation measures in accordance with contractual or extra-contractual liability.