



Labgroup

Your documents. Your data.
Our business.

REPORTING POLICY

Whistleblowing

Contents

1. Goal	2
2. Application fields	2
3. Who can report an issue.....	2
4. Definitions.....	3
5. Which violations can be reported.....	3
6. The different reporting channels.....	4
6.1 Labgroup’s (internal) reporting channel	4
6.2 The competent Authority reporting channel	5
6.3 Public disclosure	6
7. Whistleblower protection	6
8. Data protection provisions for whistleblowers	7
9. Applicable law, jurisdiction and entry into force.....	8

1. Goal

At Labgroup ('Labgroup' or the 'Company'), a number of very important policies and guidelines relating to our business practices and team members are in place. Labgroup is committed to the highest standards of ethical conduct and aims to create a safe environment in which breaches of the law can be reported without fear of reprisal.

Within this framework, in accordance with the Law of 16 May 2023 transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches or omissions of European Union law, Labgroup allows you to make a report as a whistleblower¹.

2. Application fields

A report may be made concerning information acquired in a professional context concerning violations of European Union (EU) law in key policy areas. Violations include both unlawful acts and omissions and abusive practices.

The Whistleblowing Policy allows for the safe reporting and protection of those who report an actual or potential violation of national or directly applicable or European laws by Labgroup.

Luxembourg law does not apply to:

- Alerts concerning breaches of national security.
- The authors of alerts whose relations are covered by medical secrecy or the secrecy of relations between a lawyer and his/her client, the professional secrecy to which a notary is bound, the professional secrecy to which a bailiff is bound, the secrecy of judicial deliberations, as well as by the rules on criminal proceedings.
- The exercise by workers of their right to consult their representatives or their trade unions, and protection against any unjustified prejudicial measure arising from such consultation, as well as the autonomy of the social partners and their right to conclude collective agreements.

3. Who can report an issue

People who have obtained information about violations in a professional context can be considered as a whistleblower and report violations

Especially:

- Employees (including interns and volunteers);
- Former employees (where information about security breaches or potential breaches has been collected during the employment relationship with Labgroup);
- Applicants (where breach information was collected during the recruitment process or other pre-contract negotiations);
- Contractors, sub-contractors (persons working under the supervision and direction of Labgroup);
- Suppliers (persons working under the supervision and management of Labgroup);

¹Sharepoint :

<https://labportal.labgroup.com/LMA/IMS%20Documents/Forms/Short.aspx?RootFolder=%2FLMA%2FIMS%20Documents%2F0%2DPolicies%2FInternal%20policies&FolderCTID=0x012000B4D933714F16F348B74CA0372B810197&View=%7BCB44636C%2D117B%2D44D7%2DA444%2DFC16AFB2CAAA%7D>

- Shareholders and persons belonging to the administrative, management or supervisory body of Labgroup.

Those who have knowledge of serious offences or criminal activities within Labgroup are included in the scope of the policy, including also a third party, or the subject working for one of Labgroup's suppliers and its employees, or any person who has information about the company's affairs, prepared to report what they have acquired in a work-related context.

4. Definitions

"Information on violations": information, including reasonable suspicions, concerning actual or potential violations of the law, European and Luxembourg law and/or internal policies which have occurred or are very likely to occur in the organisation in which the whistleblower works or has worked or in another organisation with which the whistleblower is or has been in contact in the course of his or her work, and concerning attempts to conceal such violations.

"Public disclosure": making information about violations available to the public.

"Alert" or "report": the oral or written communication of information on violations.

"Internal alert": the oral or written communication of information about violations within a legal entity in the private or public sector.

"External reporting": the oral or written communication of information on violations to the competent authorities.

"Anonymity" refers to a situation in which the identity of the whistleblower is not known to the services receiving the information and dealing with a case.

"Confidentiality of identity" means that the identity of the whistleblower is known to the recipient of the information, but that it is strictly confidential - in particular, to the person concerned - and is used on a strictly necessary basis.

"Whistleblower" means any natural person covered under this Policy who submits a report individually and in good faith concerning: (i) misconduct that has occurred or may occur, or (ii) attempted misconduct. Reporting information as part of the regular function or duty of a particular department does not constitute whistleblowing. Reports submitted in bad faith, particularly if based on false or misleading information will not be considered admissible; such reports constitute misconduct leading to disciplinary proceedings. In all cases, all reports are considered admissible until ruled otherwise. Information that is already fully available to the public or unsubstantiated rumours and hearsay are not admissible in the context of this policy.

5. Which violations can be reported

We have established our Whistleblower Policy to encourage people to share with us information about possible wrongdoing within our business that violates or appears to violate the law. In particular, each Labgroup employee is responsible for reporting any or all activity that may have a potential to cause harm to Labgroup as a result of an illegal, unethical violation, or appears to violate both European and Luxembourg law.

To facilitate the reporting activity, concrete examples of issues should be reported, including compliance with legal provisions, data confidentiality, information security, financial crimes or irregularities,

corruption, procurement, product compliance and customer protection, discrimination and more broadly any breach or potential breach of Luxembourg and/or European law.

Reports of matters covered by specific the internal policy covering moral and/or sexual harassment and violences should be made through the channels provided for in this internal policy.

6. The different reporting channels

To report an actual or potential breach or omission of the law, you may choose to report internally to Labgroup or externally to the competent authorities. The internal reporting channel is to be preferred depending on the circumstances.

6.1 Labgroup's (internal) reporting channel

We recognise that concerns and issues may arise in a variety of circumstances, it is important to provide all whistleblowers with an opportunity to report a breach of the through a variety of channels.

The first channel, to be favoured depending on the circumstances, known as 'internal', **is available to all Labgroup employees**, as well as to all the persons mentioned in point 3 of this policy who are in contact with the legal entity as part of their professional activities, in order to report information on violations, as specified by art. 6 of the Law of 16 May 2023. In particular, it enables reports relating to the internal management of the company to be dealt with more directly.

For example, if you have been a victim or witness of unequal treatment due to discrimination (based on ethnic origin, gender, sexual orientation, religion or beliefs, disability or age), you can use Labgroup's reporting channel.

In accordance with art. 7(2) of the Law of 16 May 2023, you may submit your notification in the three administrative languages of the country (French, German, Luxembourgish) and Labgroup also allows you to do so in English.

A secure e-mail address guaranteeing the confidentiality of the data and information shared, as well as your anonymity (if you wish), makes it easy for you to make your report. In accordance with the law, you can also choose to report a violation during a call or interview: if you wish, you can contact the people in charge of the channel directly or request an interview or call via the e-mail address dedicated to reporting or via the dedicated telephone number.

To make a report, you can write to whistleblowing@labgroup.com or call the dedicated line +352 350 222 888.

Three Labgroup employees are in charge of the reporting channel to ensure a constant presence, in the event that one of the people in charge of this channel is presumed to be the perpetrator of the reported violation, and a variety of knowledge required to process a report.

In addition, since reports made via the e-mail address can be accessed by the various people in charge of the channel, it is possible for employees or people in contact with the company to make a report using the nominative professional e-mail addresses of the competent people listed below in the event that one of the people in charge of the channel is designated as the perpetrator of the alleged acts.

Here are the three people in charge of the reporting channel:

- Séverine Créola, **Authorised Director**, screola@labgroup.com, +352 350 222 261
- Morgane Quotadamo, **Human Resources Manager**, mquotadamo@labgroup.com, +352 350 222 272

- Alessandro Baglioni, **Compliance Officer**, abaglioni@labgroup.com, +352 350 222 353

As stipulated in article 7 of the Law of 16 May 2023, after your report has been received, an acknowledgement of receipt will be sent within 7 days of receipt of the report. After this 7-day period, you will receive a reply within a reasonable delay of 3 months’.

6.2 The competent Authority reporting channel

This so-called ‘external’ **channel is made available by each organisation mentioned in the law**, for all employee, but also for any person mentioned in point 3 of this policy. In particular, it enables specific reports to be dealt with directly with the entities concerned. You may choose to use a competent authorities' reporting channel if you do not wish to use Labgroup's reporting channel, or if you feel that the results of your reporting via the company's channel are not satisfactory.

Each competent authority has its own dedicated reporting channel for the subjects it deals with specifically. You can find information about their reporting channels by clicking on the respective links in the following list or by visiting their websites.

Within the limits of their respective missions and competences, the following authorities (competent authorities) receive, directly in one of the three administrative languages² or in any other language accepted by the competent authority concerned, alerts falling within the scope of the whistleblower law:

- [La Commission de surveillance du secteur financier \(Financial sector supervisory commission\)](#);
- [Le Commissariat aux assurances \(Insurance Commission\)](#);
- [L’autorité de la concurrence \(Competition Authority\)](#);
- L’Administration de l’enregistrement, des domaines et de la TVA (Registration, Domains and VAT Administration);
- [L’Inspection du travail et des mines \(Labour and Mines Inspectorate\)](#);
- La Commission nationale pour la protection des données (National Commission for Data Protection);
- [Le Centre pour l’égalité de traitement \(Centre for Equal Treatment\)](#);
- The Ombudsman, as part of his external monitoring of places where people are deprived of their liberty;
- L’Ombudsman fir Kanner a Jugendlecher (safeguard and protection of children's rights);
- L’Institut luxembourgeois de regulation (Luxembourg Regulatory Institute);
- [L’Autorité luxembourgeoise indépendante de l’audiovisuel \(Luxembourg Independent Broadcasting Authority\)](#);
- L’Ordre des avocats du Barreau de Luxembourg et l’Ordre des avocats du Barreau de Diekirch (Luxembourg Bar Association and the Diekirch Bar Association) ;
- La Chambre des notaires (Chamber of Notaries);
- Le Collège medical (Medical College);
- L’Administration de la nature et des forêts (Nature and Forestry Administration);
- L’Administration de la gestion de l’eau (Water Management Administration);
- L’Administration de la navigation aérienne (Administration of Air Navigation);
- Le Service national du Médiateur de la consommation (National Consumer Ombudsman Service);
- L’Ordre des architectes et des ingénieurs-conseils (Order of Architects and Consulting Engineers);

² In accordance with the amended law of 24 February 1984 (French, German, Luxembourgish).

- L'Ordre des experts-comptables (Order of Chartered Accountants);
- L'Institut des réviseurs d'entreprises (Institute of Company Auditors);
- L'Administration des contributions directes (Direct Tax Administration).

When you use this reporting channel, remember to choose the authority concerned by your report. For example, choose the "Commission nationale pour la protection des données" if you wish to report that your personal data is being used and stored without complying with the laws in force.

6.3 Public disclosure

This channel of disclosure means in particular informing the press of violations or by any legitimate means of public communication and in accordance with the following paragraph.

According to art. 24 of the Act of 16 May 2023, "A person who makes a public disclosure avails of the protection provided by this Act if either of the following conditions is met:

1. The person has **first made an internal and external report**, or has made a direct external report in accordance with Chapters 2 and 4, but no appropriate action has been taken in response to the report within the period referred to in Article 7, paragraph 1, point 5°, or in Article 19, paragraph 3, point 3°;
2. The person has reasonable grounds for believing that:
 - a. the breach may **represent an imminent or obvious danger to the public interest**, such as where there is an emergency situation or a risk of irreversible harm; or
 - b. in the case of external reporting, there is **a risk of retaliation**, or the breach is unlikely to be genuinely remedied, due to the particular circumstances of the case, such as where evidence may be concealed or destroyed or where an authority may be colluding with or implicated in the breach."

7. Whistleblower protection

"As provided for by article 25 of the Law of 16 May 2023, all forms of retaliation, including threats and attempts at retaliating, are prohibited against the persons referred to in article 2, as a result of the report they have made under the terms of this law and point 3 of this Policy. The following are prohibited:

- i. suspension of an employment contract, lay-off, dismissal, non-renewal or early termination of a fixed-term employment contract or equivalent measures;
- ii. demotion or refusal of promotion;
- iii. transfer of duties, change of place of work, reduction in salary, change in working hours;
- iv. suspension of training;
- v. disciplinary measures imposed or administered, reprimand or other sanction, including a financial sanction;
- vi. failure to convert a temporary employment contract into a permanent contract, where the employee had a legitimate expectation of being offered permanent employment;
- vii. coercion, intimidation, harassment or ostracism;
- viii. discrimination, disadvantageous or unfair treatment;
- ix. negative performance evaluation or work attestation;
- x. harm, including damage to a person's reputation, particularly on social networks, or financial loss, including loss of business and loss of income;
- xi. blacklisting on the basis of a formal or informal agreement at sector or industry level, which may imply that the individual will not be able to find employment in the future at sector or industry level;

- xii. early termination or cancellation of a contract for goods or services;
- xiii. the cancellation of a licence or permit;
- xiv. referral for psychiatric or medical treatment.

Labgroup does not tolerate any form of inappropriate behaviour or conscious and voluntary violation of the law. In addition, procedures are in place for the prevention and management of bullying, sexual harassment or violence. In the event of reports concerning these subjects, we would ask you to refer to the specific procedure in force.

The Human Resources and Compliance Departments, as well as the Authorised Management, work together for the well-being of employees, partners, customers and anyone else who is in contact with Labgroup. Don't hesitate to ask for their help.

Whistleblowers may choose to remain anonymous. Anonymous reports should include a description of the breach of law with all details available to the whistleblower to enable effective assessment of the case and corrective action to be taken. Anonymous whistleblowers are also encouraged to provide the above information via the single portal for reporting breaches of law or anonymous email accounts set up for this purpose, so that the relevant people can contact them.

In the interests of a possible or ongoing investigation, a whistleblower is required not to disclose information about the report, the existence or progress of an investigation.

If a whistleblower is implicated in a breach of law and decides to come forward and report it, the person must be afforded the protection prescribed in this policy. However, such disclosure shall not exempt the whistleblower from disciplinary action.

Whistleblowers who choose to report anonymously should consider that since their identities are not known, it may not be possible for Labgroup to provide them with the protection offered by this policy.

To make a report, you can write to whistleblowing@labgroup.com or call the dedicated line +352 350 222 888 as provided in section 6.1.

8. Data protection provisions for whistleblowers

The processing of personal data under this policy shall be carried out in accordance with the principles and rules provided for in the regulations applicable to the relevant working group, in particular Regulation (EU) 2018/1725 as amended, supplemented or replaced from time to time, and the relevant opinions issued by the European Data Protection Supervisor (EDPS).

Whistleblowers shall be informed of the processing of their personal data by the relevant working group as part of the acknowledgement of receipt of the whistleblower report, and in accordance with the respective applicable procedures and shall be provided with the corresponding data protection statement. Whistleblowers shall have the right to access, rectify and (in certain circumstances) block their data by contacting the persons within Labgroup responsible for investigating their report. Restrictions to these rights may only apply in accordance with the relevant internal rules based on Article 25 of Regulation (EU) 2018/1725.

Personal data which are manifestly not relevant for the processing of a specific report shall not be collected or, if collected accidentally, shall be deleted without undue delay.



9. Applicable law, jurisdiction and entry into force

This whistleblower policy is governed by the laws of Luxembourg. Any dispute arising out of or in connection with this policy will be submitted to the courts of the city of Luxembourg which have exclusive jurisdiction. This policy has been informed to the staff delegation in accordance with Luxembourg law. The management reserves the right to adapt this policy at its discretion (subject to respecting the rights of the staff delegation in this context).