Netcompany

Whistleblower Policy

Version	3.00
Status	Approved
Issued By	Legal

© Copyright 2025 Netcompany
All rights reserved.

All industrial and intellectual property rights contained in this document are under protection of the intellectual property law and all related copyrights are reserved by Netcompany. No part of this document may be reproduced, stored in a retrieval system, or transmitted, on any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Netcompany.

Document history

Version	Date	Description	Pages
1.00	08/06/2022	Initial Version	All
2.00	18/11/2022	Specialization of the procedure for submitting, receiving and monitoring reports to public and private sector bodies.	All
3.00	08/05/2025	Content updated due to rebranding. File renamed from 'Whistleblowing Luxembourg - Policy EN' to 'SEE&EUI_Whistleblower-Policy_LU'.	All

Table of contents

1 INTRODUCTION AND PURPOSE 4

2 WHO CAN USE THE ARRANGEMENT? 4

3 WHAT MAY BE REPORTED THROUGH THE ARRANGEMENT? 5

4 INTERNAL REPORTING CHANNEL 6
4.1 Contents of the report 6
4.2 How can a report be submitted and who is to receive the report? 6

5 ANONYMITY 7

6 INFORMATION TO THE WHISTLEBLOWER 8

7 INFORMATION TO AND PROTECTION OF THE PERSON CONCERNED 8

8 PROTECTION OF THE WHISTLEBLOWER 9

9 EXTERNAL WHISTLEBLOWER SYSTEMS 10

10 PUBLIC DISCLOSURE 11

11 DATA SECURITY AND DATA STORAGE 11

12 QUESTIONS 12

13 UPDATING 12

1 INTRODUCTION AND PURPOSE

This Whistleblower Policy describes the purpose of Netcompany S.A. (hereinafter referred to as "Netcompany") having introduced a Whistleblower Arrangement (hereinafter referred to as the "**Arrangement**"), how it works, who can make use of the Arrangement, and what may be reported through the Arrangement.

The Arrangement includes the following companies:

- Netcompany S.A.

The purpose of the Arrangement is to ensure that a Whistleblower, as defined in this Whistleblower Policy, can swiftly and confidentially, through a special, independent and autonomous channel, report violations or potential violations occurring in a work-related context (and also during business trips, professional training, etc. including outside normal working hours) within the scope of the Luxembourg law of 16 May 2023 implementing Directive (UE) 2019/1937 on the protection of persons who report breaches of Union law (the "**Whistleblowing Directive**") which entered into force on 21 May 2023 (hereinafter referred to as the "**Whistleblower Law**"), allowing an independent and autonomous whistleblower unit to assess which steps are required in this respect.

The Arrangement guarantees a right to report breaches, however, reporting is not an obligation and remains optional for everyone.

2 WHO CAN USE THE ARRANGEMENT?

2.1 The Arrangement can be used by persons who report information on violations to which the person in question has gained access in connection with his or her work-related activities, and who belong to the following categories of persons (hereinafter referred to as "**Whistleblower**"):

(i) Employees or former employees and individuals in a recruitment process with the company;
(ii) Current and former Self-employed persons in business contact with the Company or in pre-contractual negotiations;
(iii) Shareholders and members of the executive management, board of directors, or similar governing body in an undertaking or non-executive members;
(iv) Volunteers;
(v) Paid or unpaid trainees;
(vi) Persons working or formerly working under the supervision and management of contracting parties, subcontractors, and suppliers and individuals involved in pre-contractual negotiations;
(vii) Persons who are reporting or publishing information to which they have gained access in a work-related relationship that has ceased since then;
(viii) Persons in work-related relationships that have not yet commenced, who report information on violations to which they have gained access during the course of the recruitment process or other pre-contractual negotiations;
(ix) Persons who assist a reporting person in the reporting process in a work- related context and are in contact with the company;
(x) Third persons who are connected with a reporting person in a work-related context and are in contact with the company;
(xi) legal entities that a reporting person owns, works for or is otherwise connected with in a work-related context and are in contact with the company.

2.2 Persons listed under section 8.5 can also file reports under the Arrangement (for instance an intermediary assisting the Whistleblower with the reporting process in a work-related context).

3 WHAT MAY BE REPORTED THROUGH THE ARRANGEMENT?

3.1 The Arrangement is open for reports regarding violations of EU law within the scope of application of the Whistleblower Directive (see section 3.4 (i)) as well as reports regarding serious offences or other serious matters (see section 3.4 (ii)).

3.2 "Violations" means acts or omissions that:

(a) are illegal or constitute a serious offence or other serious matters comprised by section 3.4; or

(b) allow circumventions of the purpose of the rules under section 3.4.

3.3 Any information may be reported, including reasonable suspicion about actual or potential violations or serious matters comprised by section 3.4 which have occurred or most probably will occur at Netcompany, as well as any attempts to cover up such violations.

3.4 The report must concern violations or potential violations within the scope of the Whistleblower Law, defined as acts or omissions which:

(i) are unlawful or are contrary to the object or purpose of directly applicable of national law, amongst others, but not limited to:

- Violation of any duty of confidentiality;
- Abuse of financial means;
- Theft;
- Deceit;
- Embezzlement; Fraud;
- Bribery;
- Any criminal offence;
- Risk or damage to the environment;
- Violation of industrial safety rules;
- Any form of sexual harassment; and
- Severe harassment, e.g. bullying, violence, and harassment due to race, political or religious affiliation.

(ii) are illegal pursuant to EU law within a number of specific areas, amongst other, but not limited to:

- Public procurement;
- Money-laundering;
- Product safety and compliance;
- Transport safety;
- Food and feed safety;
- Animal health and welfare;
- Protection of the environment;
- Public health;
- Consumer protection;
- Protection of privacy and personal data; and
- Security of network and information systems.

3.5 The Arrangement may only be used for reporting reasonable suspicions concerning actual or potential violations in relation to the issues described in section 3.4 that have occurred or most probably will occur in Netcompany's organisation, committed for instance by employees, executive management, or members of the board of directors of Netcompany. For the avoidance of doubt, this includes reasonable suspicions, concerning actual or potential violations which have occurred or are very likely to occur in the organisation in which the Whistleblower works, has worked or in another organisation with which the Whistleblower is or has been in contact in the course of their work, and concerning attempts to conceal such violations.

In connection with reports on incidents committed by Netcompany please note that such incidents may be reported although the incident cannot be attributed to an individual person but may be due to a basic systemic failure at Netcompany.

© 2025 Netcompany

4 INTERNAL REPORTING CHANNEL

Netcompany encourages the Whistleblower to report any information or reasonable suspicions obtained in the context of their employment or business relationship regarding actual or potential breach(es) which have occurred or are very likely to occur, and attempt(s) to conceal such breach(es) in accordance with section 3 of the Whistleblower Policy via an internal reporting channel.

Netcompany has set up the following procedure for the Whistleblower to make an internal report through the internal reporting channel.

Safeguards will be put in place throughout every stage of the procedure to protect against disclosure of any information that could lead to the Whistleblower identification. Netcompany's internal reporting channel is designed, set up and managed in a secure manner which guarantees the confidentiality of the identity of the Whistleblower and of any third party mentioned in a report, and which prevents access by unauthorised staff members.

4.1 Contents of the report

4.1.1 To facilitate further investigation of the reported issue, and to be able to identify the offence, it is important that the Whistleblower describes the offence in the best possible way in English, French, German or Luxembourgish as soon as the person in question becomes aware of the breach or potential breach. It is thus not possible to make any further investigations of a report if the report is not specified or if it only contains very general allegations without any further clarification.

4.1.2 Therefore, it is important that the Whistleblower - to the utmost extent - provides the following information:

- a description of the matter;
- the person(s) involved;
- whether others are aware of the suspicion about the matter;
- whether the executive management knows about the matter;
- whether documents exist that support the matter;
- whether and where further information may be found about the matter;
- for how long the matter has gone on; and
- whether the Whistleblower knows about any attempts to hide the offence.

4.1.3 Manifestly unfounded reports will not be investigated further.

4.2 How can a report be submitted and who is to receive the report?

4.2.1 Netcompany has appointed a Whistleblower Unit (as defined below) that:

(a) will receive the reports and be in contact with the Whistleblower;
(b) will follow-up on the reports; and
(c) give feedback to the Whistleblower.

4.2.2 The Whistleblower Unit in charge of the tasks mentioned in section 4.2.1. consists partly of two lawyers from Plesner Law Firm (hereinafter "**Plesner**"), and partly of an impartial group of persons at Netcompany.

4.2.3 Written reports are submitted through Plesner's Whistleblower Arrangement that can be found on

Netcompany's website and intranet: https://netcompany.com/whistleblower/.

4.2.4 Written reports are received by two lawyers at Plesner. Plesner will make a legal capacity assessment of the persons of the Whistleblower Unit who are able to process the report, after which the report will be forwarded to the relevant persons (hereinafter referred to as "**Case Managers**") at Netcompany (Plesner and the Case Managers together referred as to the "**Whistleblower Unit**"). Before forwarding the report to the Case Managers, Plesner will assess whether the report falls within the scope of application of the Arrangement.

4.2.5 It is only possible to submit written reports under the Arrangement.

4.2.6 The Whistleblower Unit will treat all written reports as confidential.

4.2.7 The Case Managers appointed to receive and follow up on the reports are subject to a duty of confidentiality regarding the information contained in the reports.

5 ANONYMITY

5.1 Netcompany encourages the Whistleblower to state his or her name when submitting a report so that the Case Managers are able to ask clarifying questions and subsequently provide feedback on the further course of the investigation. However, anonymous communication between the Whistleblower Unit and a Whistleblower who chooses to be anonymous is possible (see section 5.4 and 5.5).

5.2 If the Whistleblower chooses to submit an anonymous report, it is recommended - to ensure full anonymity - that the Whistleblower uses a private PC or, for instance, a PC located at a public library.

5.3 Plesner will make a communication module available, allowing the Whistleblower to communicate with the Whistleblower Unit for the purpose of providing additional information about the reported issue, which Plesner will then pass on to the Case Managers.

5.4 If the Whistleblower chooses to submit an anonymous report, it is possible for the Whistleblower to communicate with the Whistleblower Unit through the communication module. The Whistleblower can provide additional information to the Whistleblower Unit through the communication module and remain anonymous. In connection with the reporting, a one-off code is generated which, in order to safeguard the anonymity, cannot be re-created. Therefore, it is **important** that the Whistleblower keeps the code and remembers to log on the communication module to communicate with the Whistleblower Unit.

5.5 The communication module can be accessed through the above-mentioned link under the Arrangement (see section 4.2.3) to log on the communication module. If the Whistleblower chooses to be anonymous, it is important that the Whistleblower regularly enters the communication module to check whether the Whistleblower Unit has asked any questions. If the Whistleblower is anonymous, the Whistleblower Unit is not able to come into contact with the Whistleblower in any other ways, for instance to inform the Whistleblower that additional questions etc. have been submitted.

6 INFORMATION TO THE WHISTLEBLOWER

6.1 The Whistleblower will receive:

(a) an acknowledgement of receipt of the report within seven (7) days at the latest of that receipt; and

(b) feedback soonest possible and in principle within three (3) months from the acknowledgement of receipt of the report.

6.2 "Feedback" means a notification about the measures taken by Netcompany to assess the correctness of the allegations made in the report and, where relevant, to counter the reported offence. The feedback provided by the Whistleblower Unit must, at any time, observe the rules under data protection law, which may entail limitations in relation to the contents of the feedback to the Whistleblower.

6.3 In any case, any investigation will be conducted in accordance with the following rules:

(a) Notes will be kept of all stages of the investigation. The Case Manager(s) in charge of the investigation will offer the Whistleblower the opportunity to review and confirm the accuracy of any written summary or notes of the issue raised.
(b) The reported person(s) will be invited to meet the Case manager(s), will be given details of the allegation(s) made against them, without prejudice to the confidentiality of the Whistleblower's identity, and will be given the opportunity to respond to the allegation(s).
(c) Where witnesses are identified by either party, the Case manager(s) will use their best endeavours to investigate the matter further with such witnesses, without disclosing any information about the identities of the parties involved, to the extent legally possible.
(d) Where an investigation makes it necessary for other staff members to be interviewed, these interviews will be conducted in the strictest confidence. The need for confidentiality will be stressed to all staff involved in the investigation process and it will be made clear that any breach of confidentiality may result in disciplinary action.
(e) When the investigation into the report has been completed, a record will be made of the investigation, its outcome and any action taken, subject to compliance with GDPR and the relevant Luxembourg laws.

7 INFORMATION TO AND PROTECTION OF THE PERSON CONCERNED

7.1 After a preliminary investigation has taken place and all relevant evidence has been secured, the reported person will for instance be informed about:

(a) the identity of the Case Manager(s) responsible for the investigation of the report; and

(b) the issues of the report.

7.2 Pursuant to the Whistleblower Law, the reported person is entitled to protection of his or her identity during the case management and has a right to effective defence. These rights may not be waived by agreement to the detriment of the reported person.

7.3 Under certain circumstances, the reported person will also have the right of access to information about the Whistleblower's identity where necessary for the reported person to exercise his or her right to an effective defense (see section 8.6).

7.4 Otherwise, Netcompany observes the rights of the reported person under the GDPR. Reference is made to Netcompany's Privacy Policy for the Whistleblower Arrangement, which can be found at https://netcompany.com/whistleblower/. The Privacy Policy contains further information on the processing of personal data and the rights of the data subject.

8 PROTECTION OF THE WHISTLEBLOWER

8.1 Pursuant to the Whistleblower Law, Whistleblowers are protected against retaliation when submitting a report to the Arrangement. Such protection only applies if the following conditions are fulfilled:

(a) The person submitting the report meets the conditions to be considered a whistleblower (see section 2);
(b) The Whistleblower had reasonable grounds to believe that the reported information was correct at the time of reporting; and
(c) The reported information falls under the scope of application of the Whistleblower Law (see section 3.4).

8.2 "Retaliation" means unfavourable treatment or unfavourable consequences as a reaction to a report. This may be suspension, dismissal, demotion, or equivalent measures.

8.3 If the Whistleblower submits a report in bad faith and is fully aware of the fact that the reported information is not correct, the Whistleblower is not protected against retaliation. Depending on the circumstances, the Whistleblower can be sanctioned with a fine or imprisonment if he or she has deliberately submitted false reports. If the Whistleblower is employed by Netcompany, it may also have employment-related consequences, entailing inter alia:

(a) promotional opportunities being negatively impacted;
(b) exclusion from performance related bonuses / salary increases;
(c) formal warning (advertisement);
(d) demotion;
(e) dismissal (with or without notice);
(f) termination of business relationship; or
(g) revocation of authority (revocation ad nutum).

8.4 Netcompany also reserves the right to impose such other penalty as it considers appropriate based on the circumstances and/or to commence legal proceedings to seek, amongst others, indemnities to compensate for any harm suffered and/or criminal penalties for bad faith Whistleblowers, as described under clause 8.3, or for Whistleblowers who obtain or gain access to information in a manner which constitutes a self-standing criminal offence.

8.5 In addition to the group of persons mentioned in section 2.1, the protection described in this section 8 also applies to the following persons or entities:

(a) Intermediaries;
(b) Third parties who are connected to the Whistleblower and who risk being subject to retaliation in a work-related context (e.g. a colleague); or
(c) Undertakings and authorities which the Whistleblower owns or works for or is otherwise connected with in a work-related context (e.g. an undertaking owned by the Whistleblower).

8.6 Where necessary, information about the identity of the Whistleblower or any other information that directly or indirectly may reveal the Whistleblower's identity will only be disclosed to other persons than the Whistleblower Unit after having obtained prior explicit consent from the Whistleblower.

8.7 Prior to the disclosure of the identity of the Whistleblower, the Whistleblower will be informed accordingly and be provided with the grounds for the disclosure, unless such information would jeopardize the related investigations or judicial proceedings. Concerning the disclosure of the Whistleblower's identity, reference is also made to section 7.3.

8.8 The identity of the Whistleblower may also be revealed in connection with legal proceedings regarding the reported matter.

8.9 If the Whistleblower has deliberately revealed his or her identity in connection with a publication of the reported matter, the special considerations regarding the protection of the Whistleblower's identity are not applicable. In such cases, information on the Whistleblower's identity may be passed on pursuant to the rules under the General Data Protection Regulation.

8.10 Other information from the report, i.e. information not revealing the Whistleblower's identity, will only be disclosed to persons outside the Whistleblower Unit as part of a follow-up on the report or for the purpose of preventing a potential offence in relation to the issues described in section 3.4.

9 EXTERNAL WHISTLEBLOWER SYSTEMS

9.1 Whistleblower who intends to submit a report under Arrangement is strongly encouraged to make an internal report in accordance with section 4 to ensure the report is handled in the fastest and most efficient manner. However, Whistleblower(s) may instead choose to report any breach through the external whistleblower system of one of the twenty-two (22) competent authorities listed below:

1) La Commission de surveillance du secteur financier;
2) Le Commissariat aux assurances;
3) L'autorité de la concurrence;
4) L'Administration de l'enregistrement, des domaines et de la TVA;
5) L'Inspection du travail et des mines;
6) La Commission nationale pour la protection des données;
7) Le Centre pour l'égalité de traitement;
8) Le Médiateur dans le cadre de sa mission de contrôle externe des lieux où se trouvent des personnes privées de liberté;
9) L'Ombudsman fir Kanner a Jugendlecher;
10) L'Institut luxembourg eois de régulation;
11) L'Autorité luxembourg eoise indépendante de l'audiovisuel;
12) L'Ordre des avocats du Barreau de Luxembourg et l'Ordre des avocats du Barreau de Diekirch;
13) La Chambre des notaires;
14) Le Collège médical;
15) L'Administration de la nature et des forêts;
16) L'Administration de la gestion de l'eau;
17) L'Administration de la navigation aérienne;
18) Le Service national du Médiateur de la consommation;
19) L'Ordre des architectes et des ingénieurs-conseils;
20) L'Ordre des experts-comptables;
21) L'Institut des réviseurs d'entreprises;
22) L'Administration des contributions directes.

9.2 The Reporting Office ("Office des signalements") is the competent body in Luxembourg, should the Whistleblower require any guidance on how to report a breach.

© 2025 Netcompany

10 PUBLIC DISCLOSURE

10.1 In very limited circumstances, Whistleblower(s) may disclose a breach publicly, if:

(a) after an internal and an external report or an external report only, no appropriate action was taken within three (3) months and seven (7) days; or

(b) the Whistleblower has reasonable grounds to believe that:

(i) the breach may constitute an imminent or manifest danger to the public interest, such as an emergency situation or a risk of irreversible damage; or

(ii) in the case of an external report, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed due to the specific circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the breach perpetrator or involved in the breach.

10.2 Publicly disclosed breach(es) in violation of these clauses may incur civil liability for damage suffered by Netcompany.

11 DATA SECURITY AND DATA STORAGE

11.1 Netcompany will register all reports received under the Arrangement. The registration takes place in accordance with the provisions of the Whistleblower Law. Netcompany will store a report as long as necessary and proportionate in order to comply with the requirements imposed by law and GDPR as set out under the company's privacy policy.

11.2 Netcompany and the Whistleblower Unit will process all information reported through the Arrangement, including information on persons reported through the Arrangement, in accordance with applicable law in force at any time.

11.3 All reports will be stored properly, and it will only be possible for relevant persons of the Whistleblower Unit to access the information.

11.4 A report falling outside the scope of the Arrangement will be immediately forwarded to Netcompany's Legal Director and closed in the Arrangement.

11.5 In principle, reports will be deleted from the Arrangement 45 days after Netcompany has finalized the processing, unless Netcompany has legitimate reasons to continue the storage, e.g. if required by other legislation, or if there is reason to believe that the report may be corroborated by subsequent reports on the same issue.

11.6 If the matter is reported to the police or another authority, the report will be closed in the Arrangement immediately after the case has been closed by the authorities in question.

11.7 If - on basis of the collected data - a disciplinary sanction is implemented against the reported person, or if there are other grounds justifying and requiring the continued storage of the data on the person concerned, such data will be stored, where an employee is involved, in the employee's personnel file.

11.8 Otherwise, the information is stored in accordance with Netcompany's deletion policy.

© 2025 Netcompany

12 QUESTIONS

If you have any questions regarding this Whistleblower Policy, you are welcome to contact Tzina Prokopidou, Legal Director of Netcompany at tzina.prokopidou@netcompany.com or +30 697 33 33 220.

13 UPDATING

13.1 This Whistleblower Policy has been updated on or before: May 2025.

© 2025 Netcompany